



# Arm<sup>®</sup> Cortex<sup>®</sup>-R82AE Processor

Revision r0p1

## Technical Reference Manual

**Non-Confidential**

**Issue 04**

Copyright © 2023–2025 Arm Limited (or its affiliates). 101550\_0001\_04\_en  
All rights reserved.



# Arm® Cortex®-R82AE Processor Technical Reference Manual

This document is Non-Confidential.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.

This document is protected by copyright and other intellectual property rights.

Arm only permits use of this document if you have reviewed and accepted [Arm's Proprietary Notice](#) found at the end of this document.

This document (101550\_0001\_04\_en) was issued on 2025-03-28. There might be a later issue at <https://developer.arm.com/documentation/101550>

The product revision is r0p1.

See also: [Proprietary Notice](#) | [Product and document information](#) | [Useful resources](#)

## Start Reading

If you prefer, you can skip to [the start of the content](#).

## Intended audience

This manual is for system designers, system integrators, and programmers who are designing or programming a *System on Chip* (SoC) that uses the Cortex®-R82AE processor.

## Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

This document includes language that can be offensive. We will replace this language in a future issue of this document.

To report offensive language in this document, email [terms@arm.com](mailto:terms@arm.com).

## Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on the product, create a ticket on <https://support.developer.arm.com>.

To provide feedback on the document, fill the following survey: <https://developer.arm.com/documentation-feedback-survey>.

# Contents

<b>1. The Cortex®-R82AE processor.....</b>	<b>13</b>
1.1 About the Cortex®-R82AE processor.....	13
1.2 Features.....	14
1.2.1 Split-Lock.....	16
1.2.2 Implementing Split-Lock.....	18
1.2.3 Bus protection.....	23
1.2.4 Bus timeout.....	24
1.2.5 Livelock and deadlock detection.....	24
1.2.6 Online MBIST.....	25
1.2.7 Flop parity.....	26
1.3 Configuration options.....	26
1.3.1 Configuration parameters.....	27
1.3.2 Integration-time configuration options.....	33
1.4 Supported standards and specifications.....	35
1.5 Design process.....	37
1.6 Documentation.....	38
1.7 Product revisions.....	39
<b>2. Technical overview.....</b>	<b>40</b>
2.1 Terminology.....	40
2.2 Components.....	40
2.3 Interfaces.....	47
2.4 Functional safety and reliability.....	51
<b>3. Programmers' model.....</b>	<b>53</b>
3.1 About the programmers' model.....	53
3.2 Arm®v8-R AArch64 architecture concepts.....	53
3.2.1 Architecture requirements.....	54
3.2.2 Execution state.....	58
3.2.3 Exception levels.....	58
3.2.4 Instruction set architecture.....	60
3.2.5 Data types.....	60

3.2.6 Arm®v8-R AArch64 registers.....	60
3.2.7 Memory model.....	62
3.2.8 Security model.....	63
3.3 Advanced SIMD and floating-point.....	64
<b>4. Clocks and resets.....</b>	<b>65</b>
4.1 Clocks and clock enables.....	65
4.2 Clock domains.....	67
4.3 Resets.....	69
4.4 Resetting with PPUs.....	70
<b>5. Power management.....</b>	<b>71</b>
5.1 About power management.....	71
5.2 Voltage domain.....	71
5.3 Clock gating.....	71
5.3.1 Local and regional clock gating.....	72
5.3.2 Hierarchical clock gating.....	72
5.4 Power domains.....	74
5.5 Power mode control.....	77
5.6 Debug over powerdown.....	78
5.7 Core power modes and transitions.....	78
5.8 Core powerdown.....	83
5.9 Cluster power modes.....	84
5.10 Cluster operating modes.....	88
5.11 Cluster PPU mode transitions.....	89
5.11.1 Rules governing cluster PPU mode transitions.....	92
5.11.2 PPU mode transition behavior.....	92
5.11.3 DebugBlock power modes.....	94
5.12 Cluster powerdown.....	94
5.12.1 Transitioning in and out of coherency.....	94
5.13 Cluster power mode and core power mode dependencies.....	95
<b>6. Power and reset control with PPUs.....</b>	<b>97</b>
6.1 The Power Policy Unit.....	97
6.2 PPU operation.....	100
6.2.1 Implicit resets from PPU mode change.....	100
6.3 Utility bus accesses.....	101



6.4 Encodings for cluster power modes and operating modes.....	101
6.5 Encodings for core power modes.....	102
6.6 Programming sequences for the cluster and the core.....	103
6.6.1 Programming sequence to bring the cluster and cores from Off to On mode.....	103
6.6.2 Programming sequence to bring the cluster and cores from On to Off mode.....	104
6.6.3 Programming sequence for an interrupt controller to bring cores and cluster to On or Off mode.....	105
6.7 Explicit resetting of cluster and cores and debug recovery.....	106
6.8 ECC errors during power transitions.....	110
6.9 Implications of not having a System Control Processor.....	111
6.10 PPU and reset management register summary.....	111
<b>7. Initialization.....</b>	<b>112</b>
7.1 Initializing the Cortex®-R82AE processor.....	112
7.2 Initializing TCMs.....	114
7.2.1 Preloading TCMs.....	115
7.2.2 Preloading TCMs with ECC.....	115
7.2.3 Using TCMs from reset.....	116
7.3 Initializing LLRAM.....	117
7.3.1 Preloading LLRAM.....	117
7.3.2 Using LLRAM from reset.....	118
7.4 Disabling EL2.....	119
<b>8. Memory system.....</b>	<b>120</b>
8.1 About the memory system.....	120
8.2 TCM memories.....	124
8.3 L1 memory system.....	126
8.3.1 L1 instruction memory system.....	128
8.3.2 L1 data memory system.....	131
8.4 L2 memory system.....	138
8.4.1 L2 cache slice integration.....	139
8.4.2 L2 cache allocation policy.....	141
8.4.3 L2 cache partitioning.....	141
8.4.4 L2 cache stashing.....	143
8.4.5 L2 cache data RAM latency.....	143
8.5 LLPP manager interface.....	144
8.5.1 LLPP features.....	146

8.5.2 LLPP memory attributes.....	147
8.5.3 LLPP transfers.....	147
8.5.4 LLPP AXI transfer restrictions.....	148
8.6 SPP manager interface.....	151
8.6.1 SPP features.....	153
8.6.2 SPP memory attributes.....	154
8.6.3 SPP transfers.....	154
8.6.4 SPP AXI transfer restrictions.....	155
8.7 MM interface.....	159
8.7.1 CHI requester interface.....	160
8.7.2 AXI manager interface.....	167
8.8 LLRAM manager interface.....	173
8.8.1 LLRAM features.....	176
8.8.2 LLRAM attributes.....	177
8.8.3 LLRAM transactions.....	178
8.8.4 Support for memory types.....	180
8.8.5 LLRAM write response.....	180
8.8.6 AXI4 compatibility mode.....	181
8.8.7 LLRAM privilege information.....	181
8.9 MACP subordinate interface.....	181
8.9.1 MACP features.....	182
8.9.2 MACP attributes.....	183
8.9.3 MACP transaction types.....	183
8.10 ACELS interface.....	186
8.10.1 ACELS features.....	188
8.10.2 ACELS attributes.....	189
8.10.3 ACELS transaction types.....	190
8.10.4 TCM subordinate.....	191
8.10.5 LLRAM ACP.....	194
8.11 Utility bus.....	195
8.11.1 Utility bus accesses.....	196
8.11.2 Base addresses for system components.....	197
8.12 Direct access to internal memories.....	197
8.12.1 Direct access to L1 memory.....	198
8.12.2 Direct access to L2 and LCU memory.....	198
8.13 Exclusives and atomics support.....	199

8.14 Bus timeouts.....	201
8.15 Real-time considerations.....	204
8.15.1 Interrupt latency.....	204
8.15.2 Real-time hierarchy.....	209
8.15.3 Freedom from Interference.....	210
8.15.4 Quality of Service.....	215
<b>9. Memory management.....</b>	<b>216</b>
9.1 About the memory management.....	216
9.2 MPU.....	217
9.2.1 MPU regions.....	218
9.2.2 Virtualization support.....	227
9.2.3 MPU register access.....	229
9.3 MMU.....	230
9.3.1 TLB organization.....	231
9.3.2 TLB match process.....	233
9.3.3 Translation table walks.....	233
9.3.4 MMU memory accesses.....	234
9.3.5 Responses.....	235
9.3.6 Memory behavior and supported memory types.....	237
9.3.7 Page-based hardware attributes.....	238
<b>10. RAS Extension support.....</b>	<b>239</b>
10.1 RAS Extension support in the processor.....	239
10.2 Memory protection behavior.....	241
10.3 Bus protection behavior.....	245
10.4 Error Containment.....	246
10.4.1 Node 0: Non-ECC Memory Errors.....	246
10.4.2 Node 1: Core Memory Errors.....	247
10.4.3 Node 4: Cluster Memory Errors.....	247
10.4.4 Node 7: Core Safety Mechanism Errors.....	248
10.4.5 Node 8: Cluster Safety Mechanism Errors.....	248
10.4.6 Non-RAS Errors.....	249
10.5 Fault detection and reporting.....	249
10.5.1 Fault Handling Interrupts.....	249
10.5.2 Error Recovery Interrupts.....	250
10.5.3 Critical Error Interrupts.....	250

10.5.4 Clearing reported faults.....	250
10.6 Exceptions.....	250
10.7 Error detection and reporting.....	251
10.7.1 Node 0: Non-ECC Memory Errors.....	252
10.7.2 Node 1: Core Memory Errors.....	252
10.7.3 Node 4: Cluster Memory Errors.....	252
10.7.4 Node 7: Core Safety Mechanism Errors.....	252
10.7.5 Node 8: Cluster Safety Mechanism Errors.....	252
10.7.6 Performance monitoring.....	253
10.8 Error injection.....	253
10.9 RAS register summary.....	255
<b>11. GIC CPU interface.....</b>	<b>256</b>
11.1 About the GIC CPU interface.....	256
11.2 Disabling the GIC CPU interface.....	258
11.3 Bypassing the GIC CPU interface.....	258
11.4 GIC CPU interface register summary.....	259
<b>12. Generic Timer.....</b>	<b>260</b>
12.1 About the Generic Timer.....	260
12.2 Generic Timer functional description.....	260
12.3 Generic Timer register summary.....	260
<b>13. Debug.....</b>	<b>261</b>
13.1 About debug methods.....	261
13.2 Debug functional description.....	263
13.3 Debug register accesses.....	265
13.3.1 Processor accesses.....	265
13.3.2 Effects of resets on Debug registers.....	266
13.3.3 External access permissions to debug registers.....	266
13.3.4 Breakpoints and watchpoints.....	267
13.4 Debug events.....	267
13.4.1 Watchpoint debug events.....	268
13.4.2 Debug OS Lock.....	268
13.5 The DebugBlock.....	268
13.5.1 DebugBlock components.....	270
13.6 ECT.....	271

13.6.1 Supported debug and trace trigger events.....	272
13.6.2 CTI triggers.....	273
13.6.3 CTI register summary.....	274
13.7 Debug register summary.....	275
<b>14. PMU.....</b>	<b>276</b>
14.1 About the PMU.....	276
14.2 PMU functional description.....	277
14.3 External register access permissions to the PMU registers.....	278
14.4 PMU events.....	278
14.4.1 Core PMU events.....	278
14.4.2 Cluster PMU events.....	289
14.5 PMU interrupts.....	293
14.6 PMU register summary.....	293
<b>15. ETM.....</b>	<b>294</b>
15.1 About the ETM.....	294
15.2 ETM trace unit generation options and resources.....	295
15.3 ETM event connectivity.....	297
15.4 Operation.....	297
15.4.1 Precise TraceEnable events.....	297
15.4.2 Parallel instruction execution.....	298
15.4.3 Comparator features.....	298
15.4.4 Trace features.....	298
15.4.5 Packet formats.....	298
15.4.6 Resource selection.....	299
15.4.7 Trace flush behavior.....	300
15.4.8 Low-power state behavior.....	300
15.4.9 Cycle counter.....	301
15.4.10 Non-architectural exceptions.....	301
15.4.11 Trace synchronization.....	301
15.5 Modes of operation and execution.....	301
15.5.1 Use of the ETM main enable bit.....	302
15.5.2 Programming and reading ETM registers.....	303
15.5.3 External register access permissions.....	303
15.6 ETM register summary.....	304

<b>16. Advanced SIMD and floating-point support.....</b>	<b>305</b>
16.1 About the Advanced SIMD and floating-point support.....	305
16.2 Low-latency single-precision instructions.....	305
 <b>A. AArch64 registers.....</b>	 <b>307</b>
A.1 AArch64 register summaries.....	307
A.1.1 AArch64 Identification registers summary.....	307
A.1.2 AArch64 Generic System Control registers summary.....	308
A.1.3 AArch64 Performance Monitors registers summary.....	313
A.1.4 AArch64 System instructions summary.....	315
A.1.5 AArch64 Debug registers summary.....	322
A.1.6 AArch64 GIC system registers summary.....	323
A.1.7 AArch64 RAS registers summary.....	325
A.1.8 AArch64 Trace unit registers summary.....	326
A.1.9 AArch64 Special-purpose registers summary.....	329
A.1.10 AArch64 Generic Timer registers summary.....	330
A.1.11 AArch64 Other system control registers summary.....	331
A.2 AArch64 register descriptions.....	332
A.2.1 AArch64 Identification register description.....	332
A.2.2 AArch64 Generic System control register description.....	418
A.2.3 AArch64 Performance Monitors register description.....	752
A.2.4 AArch64 System instruction register description.....	857
A.2.5 AArch64 Debug register description.....	1070
A.2.6 AArch64 GIC register description.....	1130
A.2.7 AArch64 RAS register description.....	1229
A.2.8 AArch64 Trace register description.....	1261
A.2.9 AArch64 Special purpose register description.....	1398
A.2.10 AArch64 Generic Timer register description.....	1421
A.2.11 AArch64 other register description.....	1452
 <b>B. External registers.....</b>	 <b>1496</b>
B.1 Registers accessed over the Utility bus.....	1496
B.1.1 Register summaries for registers accessed over the Utility bus.....	1498
B.1.2 Register descriptions for registers accessed over the Utility bus.....	1503
B.2 Registers accessed over the Debug APB bus.....	1705
B.2.1 Register summaries for registers accessed over the Debug APB bus.....	1708
B.2.2 Register descriptions for registers accessed over the Debug APB bus.....	1723

<b>C. Processor UNPREDICTABLE behaviors.....</b>	<b>2285</b>
C.1 SBZ or SBO fields in instructions.....	2285
C.2 CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values.....	2286
C.3 CONSTRAINED UNPREDICTABLE behavior due to inadequate context synchronization....	2287
C.4 Translation table base address alignment.....	2287
C.5 The Performance Monitors Extension.....	2288
C.5.1 CONSTRAINED UNPREDICTABLE accesses to PMXEVTYPER_ELO or PMXEVTYPER_ELO.....	2288
C.5.2 CONSTRAINED UNPREDICTABLE accesses to PMEVCNTR<n>_ELO and PMEVTYPER<n>_ELO.....	2289
C.5.3 CONSTRAINED UNPREDICTABLE behavior caused by MDCR_EL2.HPMN.....	2289
C.6 The Activity Monitors Extension.....	2289
C.7 Syndrome register handling for CONSTRAINED UNPREDICTABLE instructions treated as UNDEFINED.....	2290
C.8 Out of range virtual address.....	2290
C.9 Mapping of non-idempotent memory locations using the Normal memory type.....	2290
C.10 Instruction fetches from Device memory.....	2291
C.11 Programming the CSSELR_EL1.Level for a cache level that is not implemented.....	2291
C.12 Crossing a page boundary with different memory types or Shareability attributes.....	2292
C.13 CONSTRAINED UNPREDICTABLE behaviors with Load-Exclusive/Store-Exclusive pairs...	2292
C.14 CONSTRAINED UNPREDICTABLE behavior for instructions.....	2293
C.14.1 LDAXP, LDNP, LDNP (SIMD&FP).....	2293
C.14.2 LDP.....	2294
C.14.3 LDP (SIMD&FP).....	2294
C.14.4 LDPSW.....	2294
C.14.5 LDR (immediate), LDRB (immediate), LDRH (immediate), LDRSB (immediate), LDRSH (immediate), LDRSW (immediate).....	2295
C.14.6 LDXP.....	2295
C.14.7 STP.....	2295
C.14.8 STLXP.....	2296
C.14.9 STLXR, STLXRB, STLXRH.....	2296
C.14.10 STR (immediate), STRB (immediate), STRH (immediate).....	2296
C.14.11 STXP.....	2297
C.14.12 STXR, STXRB, STXRH.....	2297
C.15 Out of range values of the Set/Way/Index fields in cache maintenance instructions.....	2297
C.16 Reserved values in System and memory-mapped registers and translation table entries....	2298
C.17 CONSTRAINED UNPREDICTABLE behavior in Debug state.....	2298

C.17.1 Instructions that are CONSTRAINED UNPREDICTABLE in Debug state.....	2298
C.17.2 Exiting Debug state.....	2300
C.17.3 Changing the value of EDECR.SS when not in Debug state.....	2300
C.17.4 Syndrome information on Halting Step.....	2300
C.17.5 Illegal Execution state exception.....	2301
C.17.6 Alignment constraints.....	2301
C.17.7 Cumulative error flag.....	2301
C.17.8 Restart request trigger event.....	2302
C.17.9 External debug interface accesses to registers in reset.....	2302
C.17.10 Reserved and unallocated registers.....	2302
C.17.11 External accesses to DBGBVR<n>_EL1 and DBGBCR<n>_EL1.....	2303
C.17.12 External accesses to DBGWVR<n>_EL1 and DBGWCR<n>_EL1.....	2303
C.17.13 Accessing the EDESR.....	2303
C.17.14 Accessing the CTIAPPPULSE.....	2303
C.18 RAS registers.....	2304
<b>D. Generic handler example.....</b>	<b>2305</b>
D.1 Generic handler example, part 1.....	2305
D.2 Generic handler example, part 2.....	2306
<b>Proprietary Notice.....</b>	<b>2307</b>
<b>Product and document information.....</b>	<b>2309</b>
Product status.....	2309
Revision history.....	2309
Conventions.....	2310
<b>Useful resources.....</b>	<b>2313</b>



# 1. The Cortex®-R82AE processor

This chapter provides an overview of the Cortex®-R82AE processor and its features.

## 1.1 About the Cortex®-R82AE processor

The Cortex®-R82AE processor is a mid-performance, multi-core, in-order, superscalar processor for use in real-time embedded applications. The Cortex®-R82AE processor implements the Arm®v8-R AArch64 architecture.

The Arm®v8-R AArch64 architecture is a 64-bit R-profile Arm® architecture with only AArch64 Execution state. Therefore, the Cortex®-R82AE processor does not support the AArch32 Execution state. The Cortex®-R82AE processor supports all the mandatory features from the Arm®v8.4 architecture as well as the prefetch speculation protection, the debug over powerdown, the *Reliability, Availability, and Serviceability* (RAS) Extension, and the Performance Monitors Extension.

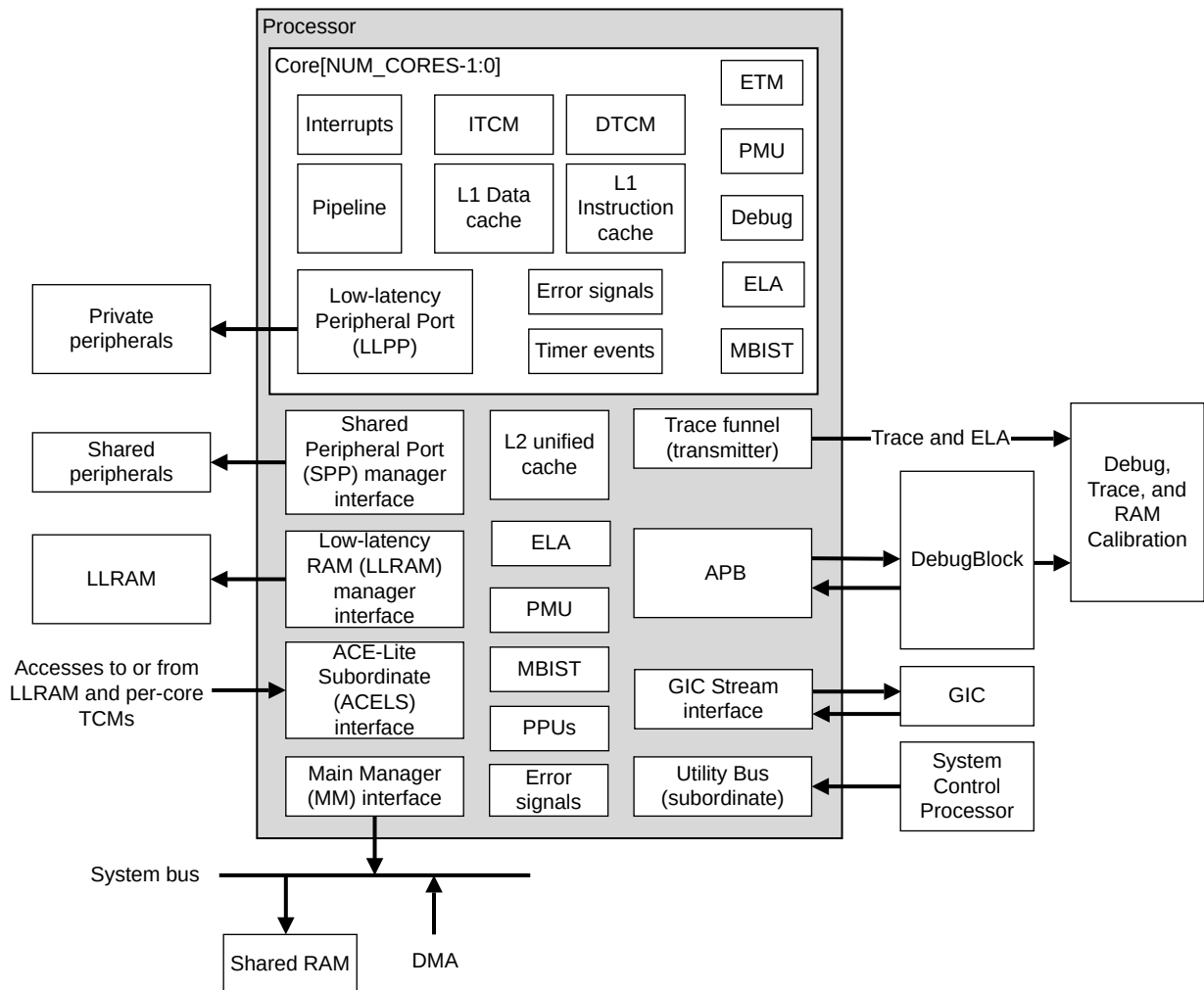
The Cortex®-R82AE processor is targeted at automotive *Advanced Driver-Assistance Systems* (ADAS) markets and similar applications that require a high level of functional safety. The Cortex®-R82AE processor has one to eight cores, each implementing a single Arm®v8-R AArch64 compliant *Processing Element* (PE). In the context of the Cortex®-R82AE processor, the PE and core are conceptually the same.

The Cortex®-R82AE processor implements Split-Lock functionality, which provides three execution modes. For example, you can use the Lock-mode for core and shared cluster logic redundancy or Split-mode for independent core execution. The Hybrid-mode is a mixed execution mode, where the cores execute independently, as in Split-mode, while the shared cluster logic executes in lock-step, as in Lock-mode.

The Cortex®-R82AE processor supports multiple *Protected Memory System Architecture* (PMSA) and *Virtual Memory System Architecture* (VMSA) contexts to execute on the same core and uses virtualization technology to isolate them in memory space. Similarly, the Cortex®-R82AE processor enables the real-time performance of different contexts to be isolated in time, which limits the impact of one context on the response time and determinism of a more critical context.

The Cortex®-R82AE processor also includes functional safety mechanisms to detect random faults that might occur in the hardware and systematic faults that might occur in the software.

The following figure shows an example Cortex®-R82AE processor system.

**Figure 1-1: Example processor system**

## 1.2 Features

The Cortex®-R82AE processor has the following features:

### Processor features

- 64-bit capability based on the Arm®v8-R AArch64 architecture.
- Up to eight cores with in-cluster and inter-cluster hardware coherency.
- Up to eight cores with in-cluster hardware coherency.
- A64 instruction set for the Arm®v8-R AArch64 architecture.
- AArch64 Execution state at EL0, EL1, and EL2 Exception levels (without EL3).
- Eight-stage, in-order superscalar pipeline with direct and indirect branch prediction.

- Support for *Protected Memory System Architecture* (PMSA) at EL1 and EL2 and optional support for *Virtual Memory System Architecture* (VMSA) at EL1.
- Secure state operation only at all Exception levels (Non-secure operation not supported).
- Compatible with Arm® TrustZone® technology, that is, support for accesses to both Secure and Non-secure physical memory address space.
- Optional *Advanced Single Instruction Multiple Data* (SIMD) and floating-point architecture support with two 64-bit data engine pipelines.
- *Generic Interrupt Controller* (GIC) CPU interface to connect to an external interrupt distributor.
- Generic Timer interface supporting 64-bit count input from an external system counter.
- Implementation of the Split, Lock, or Hybrid mode with the ability to choose an execution mode based on the CFGCEMODE input signal during Cold or Warm reset.
- 40-bit or 48-bit configurable physical address width

#### Memory system features

- Separate L1 data cache and L1 instruction cache that are private to each core.
- Two optional *Tightly Coupled Memories* (TCMs) that are private to each core, an ITCM for instructions and literal pool data and a DTCM for data.
- An optional, shared (between all cores), and unified (instructions and data) L2 cache.
- Partial L2 cache powerdown support.
- A shared CHI.E or AXI5 256-bit *Main Manager* (MM) port for instruction and data access.
- An optional and shared AXI5 256-bit *Low-latency RAM* (LLRAM) port for instruction and data access.
- A shared ACE5-Lite 128-bit *Main Accelerator Coherency Port* (MACP) for external access to MM address ranges.
- A shared ACE5-Lite 128-bit *ACE-Lite Subordinate* (ACELS) port for external access to TCMs and also LLRAM port.
- An optional and shared AXI5 64-bit *Shared Peripheral Port* (SPP) for peripheral access.
- An optional and per-core AXI5 32-bit *Low-latency Peripheral Port* (LLPP) for peripheral access.
- *Error Correcting Code* (ECC), *Single Error Correct Double Error Detect* (SECEDED) protection or *Double Error Detect* (DED) protection for all of the instantiated cache tag and data RAMs and the TCM RAMs.
- Optional bus interface protection for MM interface, LLRAM manager interface, LLPP manager interface, SPP manager interface, MACP subordinate interface, ACELS subordinate interface, and GIC AXI4-Stream interface.

#### Debug features

- Arm®v8-R AArch64 debug logic with debug over powerdown support.
- *Reliability, Availability, and Serviceability* (RAS) Extension support.
- *Embedded Trace Macrocell* (ETM), compliant with ETMv4.5, for instruction and data trace.

- Performance Monitors Extension support for software profiling and performance debugging based on the PMUv3 architecture.
- *Cross Trigger Interface* (CTI) for multiprocessor debugging.
- Optional support for integrating CoreSight™ *Embedded Logic Analyzer*, ELA-600 for advanced debug capability and signal observability. The CoreSight™ ELA-600 is a separately licensable product.
- A production *Memory Built-In Self-Test* (MBIST) for testing memories at boot time.
- Optional *Programmable MBIST Controller* (PMC) for on-line memory testing at boot time and at scheduled intervals after boot time.

### 1.2.1 Split-Lock

You can configure the Cortex®-R82AE processor to include structures to support Split-mode, Lock-mode, or Hybrid-mode, by setting the `CTMODE` configuration parameter. If the Cortex®-R82AE processor is configured to include the Split-Lock functionality, you can use the `CFGCEMODE` input to select the mode of execution at reset. This extends the functionality of a typical *Dual-Core Lock-Step* (DCLS) system by changing its execution mode on a Warm or a Cold reset.

Changing the execution mode on a Cold reset allows the Cortex®-R82AE processor to be used to build a single device for different sockets with different safety needs. Changing the execution mode on a Warm reset allows for greater debugging flexibility.

In Split-mode, the copies of the core logic operate as independent cores and there is no redundancy. Production MBIST will always force split mode behavior.

When the Cortex®-R82AE processor operates in Hybrid-mode, the copies of the core logic operate as independent cores and there is no core redundancy. However there is a redundant copy of the shared logic.

Hybrid-mode is a mixed execution mode where the cores execute independently, as in Split-mode, while the cluster executes in lock-step, as in Lock-mode. Therefore, in Hybrid-mode, the cluster provides a partial DCLS solution, with the following benefits:

- Compared to Lock-mode, Hybrid-mode offers better cluster performance, because the cores execute independently of each other.
- Compared to Split-mode, Hybrid-mode offers better cluster fault tolerance, because the cluster executes in lock-step.



From a system or software perspective, there is no difference between the Split-mode and Hybrid-mode.

---

When the Cortex®-R82AE processor operates in Lock-mode, also termed *Dual-Core Lock-Step* (DCLS) mode, both shared logic and core logic are duplicated. One of the copies of the logic in each pair functions as a redundant copy of the primary core logic.

In Lock-mode, all the inputs to the logic are duplicated and connected to both the primary logic and the redundant logic. The outputs from the two copies of the logic are then compared for errors. The cluster-level logic is also duplicated and compared. Faults that occur in either copy of the logic and cause errors on the outputs can be detected but the comparators cannot determine which copy is faulty.

Although all types of fault that cause output errors can be detected, many types of errors are masked or remain latent because they do not (or do not immediately) interfere with the operation of the Cortex®-R82AE processor.

In the Cortex®-R82AE processor implementation of Lock-mode, all the core-level and the cluster-level logic are duplicated except the RAMs and the debug logic. Instead, the RAMs are shared between the two copies of the logic and are protected by the *Error Correcting Code* (ECC) protection scheme. A separate diagnostic is provided to ensure that inadvertent activation of the debug logic are detected.



Note

The Cortex®-R82AE processor supports *Single Error Correct Double Error Detect* (SECEDED) ECC or *Double Error Detect* (DED) ECC protection scheme for *functional* RAMs. SECEDED ECC is provided for TCMs, the L1 data cache data RAMs, L1 data cache dirty RAMs, L2 cache tag and data RAMs, L2 cache data buffers, and L2 and LLRAM Coherency Unit (LCU) duplicates of L1 tag RAMs. DED ECC is provided for the L1 instruction cache data RAMs, L1 instruction cache tag RAMs, L1 data cache tag RAMs, L2 TLB data RAMs, and L2 TLB tag RAMs. L2 cache replacement RAMs and branch predictor RAMs are not protected.

The Cortex®-R82AE processor implementation of Lock-mode includes two cycles of temporal diversity between the copies of the logic. With this approach, the redundant logic operates two cycles behind the primary logic. The inputs to the redundant copy of the logic are delayed. Then the outputs of the primary and the redundant copies of the logic are captured, aligned in time, and compared. Temporal diversity provides some protection against common mode faults which can affect both copies of the logic in the same way.

The Cortex®-R82AE processor implementation of Lock-mode includes one-cycle of capture delay.

Cortex®-R82AE processor supports the following configurations:

In the following table:



Note

- MPn refers to Cortex®-R82AE processor that supports Split-mode, where n is the number of cores.
- MPnH refers to Cortex®-R82AE processor that supports Hybrid-mode, where n is the number of cores.
- MPnLS refers to Cortex®-R82AE processor that supports Lock-mode, where n is the number of cores.
- Cortex®-R82AE processor can support multiple modes depending on the value of CIMODE. For example, an MP4 / MP4H / MP2LS Cortex®-R82AE processor

can be implemented, which changes among the three modes according to the CFGCEMODE input pins.

**Table 1-1: Cortex®-R82AE processor configurations**

Configuration	Logical cores	Physical cores	Core redundancy	Cluster redundancy
MP1 (1-core cluster, Split-mode)	1	1	No	No
MP2 (2-core cluster, Split-mode)	2	2	No	No
MP3 (3-core cluster, Split-mode)	3	3	No	No
MP4 (4-core cluster, Split-mode)	4	4	No	No
MP5 (5-core cluster, Split-mode)	5	5	No	No
MP6 (6-core cluster, Split-mode)	6	6	No	No
MP7 (7-core cluster, Split-mode)	7	7	No	No
MP8 (8-core cluster, Split-mode)	8	8	No	No
MP1H (1-core cluster, Hybrid-mode)	1	1	No	Yes
MP2H (1-core cluster, Hybrid-mode)	2	2	No	Yes
MP3H (1-core cluster, Hybrid-mode)	3	3	No	Yes
MP4H (1-core cluster, Hybrid-mode)	4	4	No	Yes
MP5H (1-core cluster, Hybrid-mode)	5	5	No	Yes
MP6H (1-core cluster, Hybrid-mode)	6	6	No	Yes
MP7H (1-core cluster, Hybrid-mode)	7	7	No	Yes
MP8H (1-core cluster, Hybrid-mode)	8	8	No	Yes
MP1LS (2-core cluster, Lock-mode)	1	2	Yes	Yes
MP2LS (4-core cluster, Lock-mode)	2	4	Yes	Yes
MP3LS (6-core cluster, Lock-mode)	3	6	Yes	Yes
MP4LS (8-core cluster, Lock-mode)	4	8	Yes	Yes

## 1.2.2 Implementing Split-Lock

The R82AE processor uses a specific Split-Lock implementation to enable the cluster to execute in either Split-mode, or Lock-mode, or the mixed execution Hybrid-mode. Use the CFGCEMODE input to select the required execution mode on a Warm or a Cold reset.

The R82AE processor Split-Lock implementation only duplicates logic which is related to the function of the processor. There are no redundant copies of the debug or trace logic. However, unexpected activity in the debug logic will be detected as a fault. This fault is signaled separately from other faults, allowing to debug the processor when in Hybrid-mode or Lock-modes.

In the R82AE processor Split-Lock implementation, RAMs are not duplicated. The RAMs are shared between the two copies of the logic. In Lock-mode (and also Hybrid-mode for cluster units), both primary and redundant logic inputs are connected to the same RAM instances. The RAM instances inputs will be connected to outputs of the primary logic. This strategy increases the processor

availability, because when a correctable memory error is detected by the RAM protection logic, the processor corrects the error without producing a comparator mismatch.

In Split-mode (and also Hybrid-mode for the cores), each independent logic is connected to its own RAM instances.



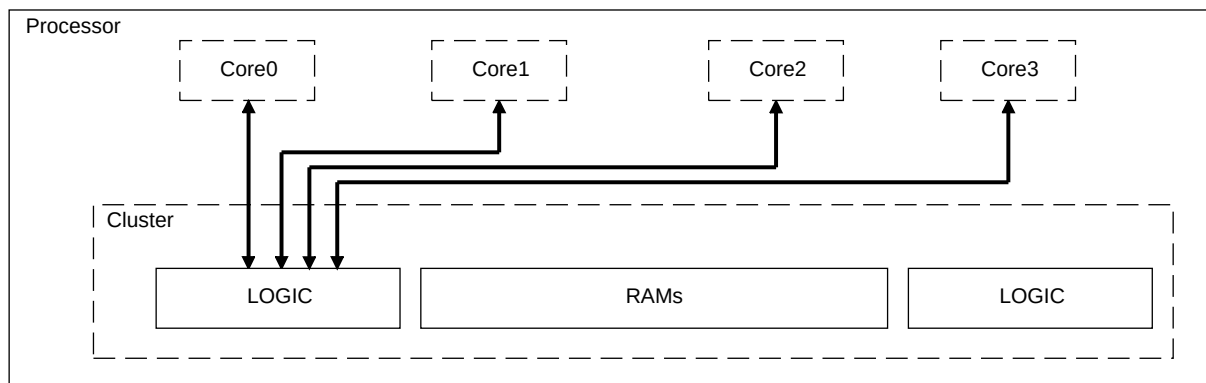
For systems that tie off CFGCEMODE to an always Lock-mode (0b11), half of the per-core RAMs are unused, with the exception of *Tightly Coupled Memories* (TCMs) that can be accessed. Such systems are expected not to integrate any unused RAMs.

RAM sharing in this way saves significant area and improves the *Failure In Time* (FIT) rate. The *Error Correcting Code* (ECC) protection scheme is always available for all functional R82AE RAMs.

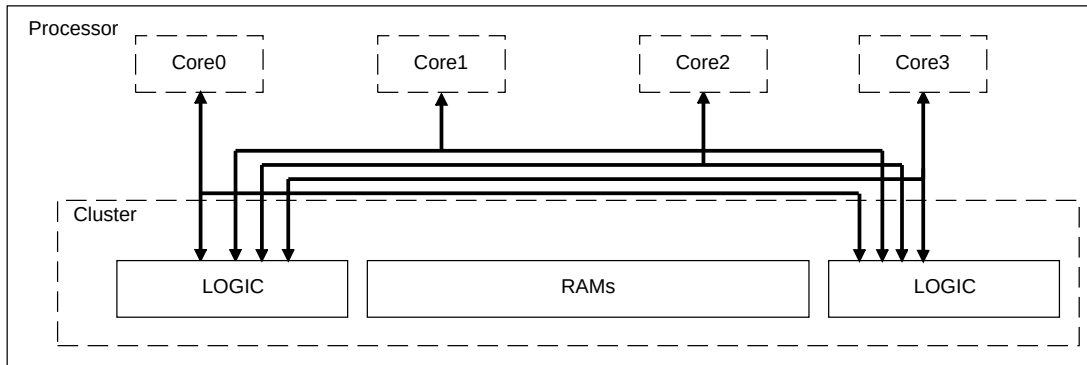
The R82AE uses a comparator with a registered output. In addition to the signals to be compared, the comparator includes a force input, and an enable that controls whether the compare generates an error. The force input can artificially force the comparator to generate an error result, to exercise the error reporting logic. To help protect against failures in the comparator, there are redundant copies of each of the comparators.

The following figure shows the R82AE processor Split-mode operation, that is, where CFGCEMODE = 0b01.

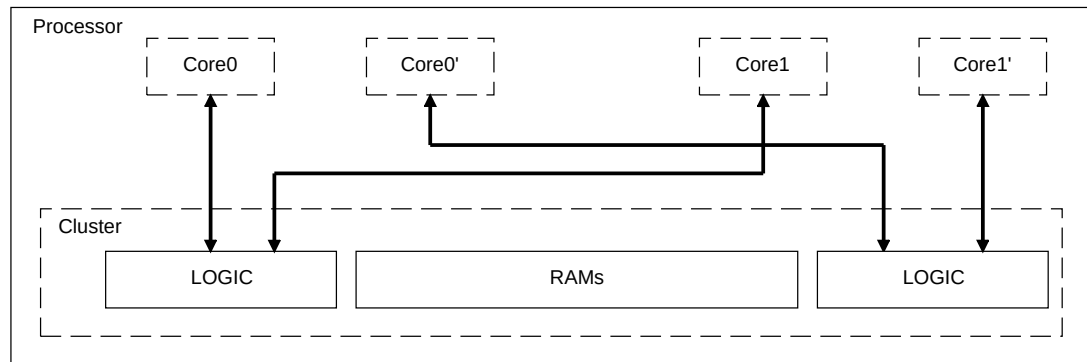
**Figure 1-2: R82AE processor Split-mode operation**



The following figure shows the R82AE processor Hybrid-mode operation, that is, where CFGCEMODE = 0b10.

**Figure 1-3: R82AE processor Hybrid-mode operation**

The following figure shows the R82AE processor Lock-mode operation, that is, where `CFGCEMODE = 0b11`.

**Figure 1-4: R82AE processor Lock-mode operation**

If the Lock-mode is implemented (`CIMODE` configuration parameter set to 2 or 3), only configurations with an even number of cores from two to eight (2, 4, 6, or 8) are supported. This is because the Lock-mode requires core pairs. Also, all the core pairs must execute in the same mode because mixed-mode execution between the core pairs is not supported. For instance, one core pair cannot execute in Lock-mode, while another core pair executes in Split-mode.

If the Lock-mode is implemented, the configuration options for the individual cores are restricted, that is the configuration of any two cores (in Split-mode and Hybrid-mode) that might be a redundant pair (in Lock mode) must be identical.



**Note**

A core pair is defined as a pair of primary and redundant cores which, when running in Lock-mode, the cluster views architecturally as a single core.

In Lock-mode, half of the cores function as redundant copies of the other cores. For example, if the number of cores is 4, two cores are logically observable. The other two cores are physically present but function as redundant copies.

Although physically present, the external inputs and outputs that are associated with the redundant cores are disabled and must not be used in Lock-mode.

For R82AE processor configurations that do not require the Lock-mode (CIMODE configuration parameter set to 0 or 1), the R82AE processor supports from one to eight cores.

In Split-mode, all external inputs and outputs associated to the physical cores are enabled, but redundancy checking is not possible.

The Cortex®-R82AE processor can be implemented to include structures to support Split-mode, Lock-mode, or Hybrid-mode, depending on the CIMODE configuration parameter. Based on the implemented mode, redundant cluster units are included or cores are arranged in redundant pairs along with redundant cluster units. The execution mode is selected among the implemented modes according to the value of CFGCEMODE input pins. Because a failure in this input would represent a significant diagnostic impact, the Cortex®-R82AE processor has CFGCEMODECHK inputs with odd parity of the CFGCEMODE signal. The parity input is always present when Hybrid-mode or Lock-mode are supported.

The number of allowed {CFGCEMODE, CFGCEMODECHK} signal combinations is limited, and any wrong value will result in the safest available mode depending on the CIMODE to be picked. The following table shows the CIMODE parameter and {CFGCEMODE, CFGCEMODECHK} signal combinations:

**Table 1-2: Combinations of CIMODE parameter and DCLS configuration signals**

Implementation mode with CIMODE parameter	Execution mode select with {CFGCEMODE, CFGCEMODECHK} signals				Illegal default
	Lock-mode	Hybrid-mode	Split-mode	Others	
0: Split-mode (No DCLS)	N/A	N/A	N/A	N/A	N/A
1: Split-mode or Hybrid-mode	Illegal	{0b10, 0b01}	{0b01, 0b10}	Illegal	Hybrid-mode
2: Split-mode or Lock-mode	{0b11, 0b00}	Illegal	{0b01, 0b10}	Illegal	Lock-mode
3: Split-mode, Hybrid-mode, or Lock-mode	{0b11, 0b00}	{0b10, 0b01}	{0b01, 0b10}	Illegal	Lock-mode

The following tables show how an 8-core cluster maps physical and logical cores in Split-mode, Hybrid-mode, and Lock-mode. In Split-mode and Hybrid-mode software would see 8 cores, whilst in Lock-mode software would see 4 cores. The tables show an MP8 cluster (in Split-mode), or an MP8H cluster (in Hybrid-mode) or an MP4LS cluster (in Lock-mode). Depending on the configuration option CIMODE, a subset of these is available to be selected by the CFGCEMODE pins. For example, only MP8 is available for Split-only configurations (CIMODE = 0), MP8 and MP8H

for Split-mode and Hybrid-mode ( $CIMODE = 1$ ), MP8 and MP4LS for Split-mode and Lock-mode ( $CIMODE = 2$ ), and MP8, MP8H, MP4LS for Split-mode, Hybrid-mode, and Lock-mode configurations ( $CIMODE = 3$ ). In the following tables:

- Physical core refers to the piece of hardware logic which implements a CPU core.
- Logical core describes how a physical core behaves according to the mode of operation. In Split-mode and Hybrid-mode, the logical cores operate independently of one another. In Lock-mode, logical cores are organized in pairs. Even-numbered physical cores become the primary logical cores, and odd-numbered physical cores become the redundant logical cores. Primary and redundant logical core outputs are compared for correctness.

**Table 1-3: Core behavior in Split-mode and Hybrid-mode for an 8 core cluster**

Split-mode or Hybrid-mode								
Physical core number	0	1	2	3	4	5	6	7
Core operation	Independent	Independent	Independent	Independent	Independent	Independent	Independent	Independent
Logical core number	0	1	2	3	4	5	6	7
MPIDR_EL1.Aff1 view for software running on the core	0	1	2	3	4	5	6	7
Mapping of core LLPP pins	ARVALIDP0	ARVALIDP1	ARVALIDP2	ARVALIDP3	ARVALIDP4	ARVALIDP5	ARVALIDP6	ARVALIDP7
Mapping of legacy interrupts, GICCDISABLE = 1	nIRQ[0]	nIRQ[1]	nIRQ[2]	nIRQ[3]	nIRQ[4]	nIRQ[5]	nIRQ[6]	nIRQ[7]
Mapping of GIC stream IDs, GICCDISABLE = 0	0	1	2	3	4	5	6	7
Mapping of GIC power management	COREWAKER	COREWAKER	COREWAKER	COREWAKER	COREWAKER	COREWAKER	COREWAKER	COREWAKER
Mapping of PPU Core P channels	0	1	2	3	4	5	6	7
Mapping of CTI interrupts	CTIIRQ[0]	CTIIRQ[1]	CTIIRQ[2]	CTIIRQ[3]	CTIIRQ[4]	CTIIRQ[5]	CTIIRQ[6]	CTIIRQ[7]
Utility bus core offsets (PPU, RAS, MBIST)	0	1	2	3	4	5	6	7
Debug APB core offsets (Debug, CTI, Trace, PMU, ELA)	0	1	2	3	4	5	6	7



In the following table, the logical cores are numbered with numerals and the redundant cores are numbered with 0', 1', 2', or 3'.

**Table 1-4: Core behavior in Lock-mode for an 8 core cluster**

Lock-mode								
Physical core number	0	1	2	3	4	5	6	7
Core operation	Primary	Redundant	Primary	Redundant	Primary	Redundant	Primary	Redundant
Logical core number	0	0'	1	1'	2	2'	3	3'
MPIDR_EL1.Aff1 view for software running on the core	0		1		2		3	
Mapping of core LLPP pins	ARVALIDP0		ARVALIDP2		ARVALIDP4		ARVALIDP6	
Mapping of legacy interrupts (GICCDISABLE = 1)	nIRQ[0]		nIRQ[1]		nIRQ[2]		nIRQ[3]	
Mapping of GIC stream IDs (GICCDISABLE = 0)	0		1		2		3	
Mapping of GIC power management	COREWAKEREQUEST[0]		COREWAKEREQUEST[1]		COREWAKEREQUEST[2]		COREWAKEREQUEST[3]	
Mapping of CTI interrupts	CTIIRQ[0]		CTIIRQ[1]		CTIIRQ[2]		CTIIRQ[3]	
Utility bus core offsets (PPU, RAS, MBIST)	0		2		4		6	
Debug APB core offsets (Debug, CTI, Trace, PMU, ELA)	0		2		4		6	

### 1.2.3 Bus protection

You can configure the Cortex®-R82AE processor to include structures to support Bus protection.

Safe systems may require protection for faults which can occur in the wiring or interconnect logic between the processor and the connected logic in the system. While protection of interconnect or system components is beyond the scope of the Cortex®-R82AE processor, Cortex®-R82AE includes an optional bus protection feature designed to protect the link between the ports on the processor and the connected interconnect or system components.

The Cortex®-R82AE processor optionally implements parity protection for all external signaling, both inputs and outputs, expected to be used during safety critical operation. This includes the primary AMBA interfaces as well as functional pins such as interrupts, configuration pins, power control and fault reporting. The excluded interfaces are associated with debug and trace which are not expected to be used during safe operation.

This feature can be configured for all interfaces of the Cortex®-R82AE processor by setting the compile-time BUS\_PROTECTION parameter to 1 (enabled) or 0 (disabled).

Cortex®-R82AE implements protocol-defined parity protection scheme where these are defined. This includes:

- AXI5: LLRAM, MM-AXI5, SPP, LLPP, Utility Bus
- CHI.e: MM-CHI.e
- ACE5-Lite: MACP, ACELS
- AXI5-Stream: GIC
- P-Channels
- Q-Channels

All other signaling is protected via odd parity in groups of up to 8 bits per parity bit.

The scheme enables detection of errors that occur on the signals being transmitted across the bus, for example, where a 32-bit data word has one bit corrupted somewhere between source and destination. The errors include faults that occur on the wires between various components or faults that might occur on the logic within the interconnect responsible for routing the signals. The scheme can also detect multi-bit errors if they occur in different parity signal groups.

For more information please refer to the Cortex®-R82AE Safety Manual.

## 1.2.4 Bus timeout

You can configure the Cortex®-R82AE processor to enable Bus timeout.

Cortex®-R82AE includes a bus timeout feature in order to detect when the Main Manager, LLRAM, SPP or LLPP interface does not respond within a programmable time limit. When a transaction presented on a manager port fails to complete, that is, a response is not received within a programmable time limit a timeout error is raised via the RAS error records.

A bus timeout error is also reported to RAS if the manager port is experiencing incoming traffic which is not serviced (with external requests) within the programmed time limit because of the clock being gated. It follows that a bus timeout error can be observed even without any traffic registered at the external manager port interface.

For more information please refer to [8.14 Bus timeouts](#) on page 201.

## 1.2.5 Livelock and deadlock detection

The Cortex®-R82AE includes livelock and deadlock detection features.

### 1.2.5.1 Livelock detection

The Cortex®-R82AE includes livelock detection features.

The livelock detector is primarily intended to detect livelock conditions that result from hard errors in Caches and RAMs implemented within the Cortex®-R82AE processor. Many instances of correctable errors require the access to be repeated in order to obtain the corrected data. While Cortex®-R82AE includes hard error protection mechanisms in order to enable forward progress

in the presence of a number of hard errors, if the capacity is exceeded a livelock may occur. The Cortex®-R82AE processor detects such livelocks and reports the error to the RAS error records. In this situation, it is possible to interrupt the core if the interrupt is not masked.

The livelock detection mechanism also detects certain software or system faults that cause the processor to livelock. These include an aborting instruction placed at the abort vector address.

The livelock detection mechanism is always included and enabled.

### 1.2.5.2 Deadlock detection

The Cortex®-R82AE includes Deadlock detection features.

The deadlock detection feature targets two key areas.

The architecture defines that interrupt masks are automatically set in hardware when an interrupt is entered. This might lead to deadlock if software fails to clear the interrupt masks to re-enable interrupts. Each Cortex®-R82AE core includes a counter for detecting when the core has been running with interrupts masked and reports a timeout to the RAS error records, if the limit is exceeded.

The same per-core counter can be used to guard against a different kind of error. When a core executes WFI/WFE instruction it will stop executing and, if possible, gate its own clock. If the appropriate wake-up event is not received, it will remain in this state indefinitely. The counter will count for how long a core is stuck executing a WFI/WFE instruction and report a timeout to the RAS error records, if the limit is exceeded.

These counters are always included and are configured and enabled through the Interrupt Monitoring Register (IMP\_INTMONR\_EL1).

### 1.2.6 Online MBIST

You can configure the Cortex®-R82AE processor to include Online MBIST features.

The Cortex®-R82AE processor optionally supports online Memory Built-in Self Test (MBIST). Online MBIST can be performed at boot time and can also be used to schedule regular testing and is capable of testing both the ECC logic and testing for latent faults in the RAMs themselves.

For each of the attachment points for production MBIST, Cortex®-R82AE will optionally provide a programmable MBIST controller (PMC-100) that can perform online MBIST, configured via the PMC parameter. The Online MBIST controller is programmable externally via the utility bus.

For more information on the PMC-100 Programmable MBIST Controller and the programmer's model please refer to the PMC-100 Technical Reference Manual.

The user is responsible to keep power ON and disable dynamic transitions during PMC programming and Online MBIST test execution. Please refer to the Cortex®-R82AE Processor Configuration and Integration Manual for further the implemented logical memory arrays.

## 1.2.7 Flop parity

The Cortex®-R82AE processor can be configured to include flop parity features.

The Cortex®-R82AE processor optionally supports flop parity in order to provide protection against transient faults in the logic. This functionality may also be referred to as Transient Fault Protection. Flop parity is expected to be used primarily in implementations which do not make use of LOCK mode, since lockstep also provides protection against transient faults in the logic.

Flop parity, if included, adds parity checks for groups of common-enabled registers in the design. Parity is calculated on the inputs to groups of registers and the parity bit is captured in an additional register. The output of the group of registers is used to recalculate the parity bit and compare it against the captured parity bit.

If a mismatch is observed then a flop parity fault has occurred and this will be reported via a dedicated per-core pin CORETFPFAULT as well as reporting the information to the RAS error records.

The flop parity functionality will be optionally embedded in the design itself under the parameter `FLOP_PARITY`. The Cortex®-R82AE processor supports flop parity protection of the core only; the cluster will not be protected as implementations targeting ASIL-B are expected to make use of Hybrid lock, which protects the cluster from transient errors in the logic. Implementations targeting ASIL-D are not expected to implement flop parity, however Cortex®-R82AE permits flop parity to be configured even where split/lock is implemented; a given system might be targeting ASIL-D in lockstep, but still wish to operate at ASIL-B when running in split within a single implementation.

It is not possible to enable/disable the flop parity logic during runtime - if `FLOP_PARITY` is configured then it is always active, as the area and timing cost of implementing a pin or flop-based enable for all of the parity flops is prohibitive. Instead, it is possible to enable or disable the reporting of flop parity failures to RAS and CORETFPFAULT via the `IMP_MEMPROTCTLR_EL1.TFPEN` control. The reset value of this register control is pin configurable via `CFGTFPEN`, such that flop parity reporting can be enabled or disabled out of reset. If a flop parity fault occurs in a lockstep implementation then a DCLS divergence will occur as a result of the CORETFPFAULT pin, and on any read of the RAS status.

For more information please refer to the Cortex®-R82AE Safety Manual.

## 1.3 Configuration options

You can configure the Cortex®-R82AE processor during the rendering and integration stages to meet your functional requirements.

To configure the Cortex®-R82AE processor, you must decide the values of:

- Configuration parameters when the Cortex®-R82AE processor RTL is rendered before the implementation.
- Top-level configuration inputs when the Cortex®-R82AE processor is integrated in the system after the implementation.

**Note**

All top-level configuration inputs are sampled in the PERIPHCLK domain, just after the Cortex®-R82AE processor comes out of Cold processor reset.

### 1.3.1 Configuration parameters

The configuration parameters affect the global and per-core RTL parameters.

Global parameters apply to the entire cluster while per-core parameters can be configured differently for different cores within the cluster.

**Note**

When CIMODE is set to 2 or 3, for all the per-core parameters, the value of per-core-instance parameter for odd-numbered core logic instances must be the same as those for the other core instance in the core instance pair.

Some memories and interfaces are optional so that you can configure the memory system according to your system requirements. When you choose to exclude:

- An optional memory:
  - For the *Instruction Tightly Couple Memory* (ITCM) and *Data Tightly Coupled Memory* (DTCM), the logic is removed.
  - For the L2 memory, the logic is always present but the RAM size is 0.
- An optional interface, the logic is removed.

The following table shows the main configuration parameters.

To successfully use a Cortex®-R82AE processor core configured without Advanced SIMD and floating-point support (`NEON_FP<m> = 0`), you must ensure that software binaries running on this core do not use any Advanced SIMD or floating-point instructions. Advanced SIMD or floating-point instructions can be introduced in a number of ways. For example:

**Warning**

- By explicitly using them in assembly code.
- By using float or double data types or SIMD intrinsics in C or other high-level languages.
- By the compiler if Advanced SIMD/floating-point code generation is not disabled (such as auto-vectorization flags are enabled).
- By software libraries that are linked either explicitly by the user or implicitly by the compiler (independently of whether Advanced SIMD/floating-point code generation is enabled for the source being compiled). For further information, please refer to: <https://developer.arm.com/documentation/ka005579/latest>

**Table 1-5: Configuration parameters**

Parameter name	Scope	Permitted values	Description
NUM_CORES	Global	1, 2, 3, 4, 5, 6, 7, 8 if CIMODE is 0 or 1  2, 4, 6, 8 if CIMODE is 2 or 3	Controls the number of physical cores
CHI	Global	0, 1	Controls the type of protocol the <i>Main Manager</i> (MM) interface implements  <b>0</b> MM interface is AXI <b>1</b> MM interface is CHI
BUS_PROTECTION	Global	0, 1	Controls the inclusion of structures that are required to support bus protection functionality  <b>0</b> Not included <b>1</b> Included, buses are parity protected
FLOP_PARITY	Global	0, 1	Provides protection against transient faults in the logic in implementations targeting ASIL-B  <b>0</b> Flop parity is not configured <b>1</b> Flop parity included for all cores
ADDR_FOLD	Global	0, 1	Controls the inclusion of address bits in the memory protection (ECC, EDC) schemes  <b>0</b> RAM address bits not included in memory protection <b>1</b> RAM address bits included in memory protection
PMC	Global	0, 1	Controls the inclusion of <i>Programmable MBIST Controller</i> (PMC) to support PMC-100 functionality.  <b>0</b> Not included <b>1</b> Included
PMC_P_REG	Global	4 - 32	Configures the number of program register available in the PMC. See the Arm PMC-100 Technical Reference Manual for more information.
ELA	Global	0, 1	Controls the inclusion of the CoreSight™ <i>Embedded Logic Analyzer</i> , ELA-600  <b>0</b> Not included <b>1</b> Included  <b>Note:</b> The ELA-600 is a separately licensable product
ELA_ATB_FIFO_DEPTH	Global	4, 8, 16, 32, 64	Configures the ELA-600 ATB FIFO depth in powers of two. See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a> for more information.



Parameter name	Scope	Permitted values	Description
L2_CACHE_SIZE	Global	0, 96, 128, 192, 256, 384 512, 768, 1024, 1536, 2048, 3072, 4096	Controls the size of the L2 cache  0: L2 cache logic is present but RAM size is 0  96: 96KB cache  128: 128KB cache  192: 192KB cache  256: 256KB cache  384: 384KB cache  512: 512KB cache  768: 768KB cache  1024: 1024KB cache  1536: 1536KB cache  2048: 2048KB cache  3072: 3072KB cache  4096: 4096KB cache
L2_DATA_WR_LATENCY	Global	0, 1, 2	L2 cache data RAM input latency  <b>0</b> 1 cycle input delay from L2 data RAMs  <b>1</b> 2 cycles input delay from L2 data RAMs  <b>2</b> 2 cycles input delay plus 1 cycle hold from L2 data RAMs
L2_DATA_RD_LATENCY	Global	0, 1	L2 cache data RAM output latency  <b>0</b> 2 cycles output delay from L2 data RAMs  <b>1</b> 3 cycles output delay from L2 data RAMs
L2_DATA_RD_SLICE	Global	0, 1	L2 cache data RAM output register slice  <b>0</b> No register slice <b>1</b> Register slice included
L2_DATA_STRETCH_CLK	Global	0, 1	L2 cache data RAMs clock pulse stretch  <b>0</b> Not stretched <b>1</b> Stretched

Parameter name	Scope	Permitted values	Description
L2_SLICES	Global	1, 2	Controls the number of slices and RAM partitions the L2 cache implements <b>1</b> The L2 cache implements a single slice and a single RAM partition <b>2</b> The L2 cache implements two slices and two RAM partitions
CPU_SLICE	Global	0, 1	Controls whether extra register slices exist between the cores and the cluster logic <b>0</b> No additional register slices exist between the cores and cluster logic <b>1</b> One additional register slice exists between the cores and cluster logic <b>Note:</b> Depending on your target frequency, setting CPU_SLICE to 1 may help with the timing closure.
CIMODE	Global	0, 1, 2, 3	Controls the inclusion of structures required to support Split, Lock, Hybrid modes in the processor <b>0</b> Does not include structures required to support Lock-mode or Hybrid-mode <b>1</b> Includes structures required to support either Split-mode or Hybrid-mode <b>2</b> Includes structures required to support either Split-mode or Lock-mode <b>3</b> Includes structures required to support Split-mode, Lock-mode, or Hybrid-mode
PPU_RST_STATE	Global	0, 1	Power on reset state for the <i>Power Policy Units</i> (PPUs) <b>0</b> Cluster and all core PPUs reset to off <b>1</b> Cluster and all core PPUs reset to on
ACELS_ID_WIDTH	Global	Any integer value between 8 and 24	Defines the width of the <i>ACE-Lite Subordinate</i> (ACELS) port ID signals AWIDS, BIDS, ARIDS, and RIDS.
MACP_ID_WIDTH	Global	Any integer value between 8 and 24	Defines the width of the <i>Main Accelerator Coherency Port</i> (MACP) ID signals AWIDA, BIDA, ARIDA, and RIDA.
UB_ID_WIDTH	Global	Any integer value between 1 and 24	Defines the width of the <i>Utility bus</i> port ID signals AWIDU, BIDU, ARIDU, and RIDU.

Parameter name	Scope	Permitted values	Description
LLPP	Global	0, 1	Controls the existence of cores' <i>Low-latency Peripheral Port</i> (LLPP)  <b>0</b> No LLPP regions and ports exist. All related AXI inputs and outputs as well as the CFGLLPPIMP and CFGLLPPBASEADDR pins are rendered out by the configuration script  <b>1</b> All cores include logic to support LLPP regions and ports. They can be enabled or disabled by the CFGLLPPIMP pin
SPP	Global	0, 1	Controls the existence of the cluster <i>Shared Peripheral Port</i> (SPP)  <b>0</b> No SPP region and port exists. All related AXI inputs and outputs as well as the CFGSPPIMP and CFGSPPBASEADDR pins are rendered out by the configuration script  <b>1</b> The processor includes logic to support the SPP region and port. It can be enabled or disabled by the CFGSPPIMP pin
LLRAM	Global	0, 1	Controls the existence of the cluster <i>Low-latency RAM</i> (LLRAM) interface  <b>0</b> No LLRAM region, port and coherency logic exists. All related AXI inputs and outputs as well as the CFGLLRAMSHARED, BROADCASTATOMICL, CFGLLRAMIMP, CFGLLRAMEN and CFGLLRAMBASEADDR pins are rendered out by the configuration script  <b>1</b> The processor includes logic to support the LLRAM region, port, and coherency. It can be enabled or disabled by the CFGLLRAMIMP pin and its behavior out of reset can be further defined by the CFGLLRAMEN pin
DENSE_CS_ADDR_MAP	Global	0, 1	Controls how CoreSight™ components are mapped in the Utility bus and the Debug port  <b>0</b> Sparse memory map. Each component occupies 64KB. The Utility bus has 23-bit address signals. The Debug port has 24-bit address signals  <b>1</b> Dense memory map. Each component occupies 4KB. The Utility bus has 18-bit address signals. The Debug port has 18-bit address signals
PA_W	Global	40, 48	Controls the Physical Address width 40: 40-bit physical address 48: 48-bit physical address
NUM_EL2_MPU_REGIONS<m>	Per-core	0, 16, 32	Controls the number of EL2 <i>Memory Protection Unit</i> (MPU) regions. <m> is the core number
NUM_EL1_MPU_REGIONS<m>	Per-core	0, 16, 32	Controls the number of EL1 MPU regions. <m> is the core number.  Value 0 is only supported when the core instance includes support for <i>Virtual Memory System Architecture</i> (VMSA).
NEON_FP<m>	Per-core	0, 1	Controls the inclusion of Advanced SIMD and floating-point support. <m> is the core number.  <b>0</b> No Advanced SIMD and no floating-point support included <b>1</b> Advanced SIMD and half-precision, single-precision, and double-precision floating-point functionality included

Parameter name	Scope	Permitted values	Description
LOW_LATENCY_SP<m>	Per-core	0, 1	Controls the inclusion of an additional single-precision floating-point pipeline which has lower result latencies than the default floating-point pipeline. <m> is the core number.  <b>0</b> Default floating-point pipeline only <b>1</b> Low-latency single-precision pipeline included
VMSA<m>	Per-core	0, 1	Controls the inclusion of VMSA functionality. <m> is the core number.  <b>0</b> Not included <b>1</b> Included
L1_ICACHE_SIZE<m>	Per-core	16, 32, 64, 128	Controls the size of the L1 instruction cache. <m> is the core number.  16: 16KB cache  32: 32KB cache  64: 64KB cache  128: 128KB cache
L1_DCACHE_SIZE<m>	Per-core	16, 32, 64	Controls the size of the L1 data cache. <m> is the core number.  16: 16KB cache  32: 32KB cache  64: 64KB cache
ITCM_SIZE<m>	Per-core	0, 16, 32, 64, 128, 256, 512, 1024	Controls the size of the <i>Instruction Tightly Coupled Memory</i> (ITCM). <m> is the core number.  0: ITCM logic is removed and RAM size is 0  16: 16KB cache  32: 32KB cache  64: 64KB cache  128: 128KB cache  256: 256KB cache  512: 512KB cache  1024: 1024KB cache
ITCM_WAIT<m>	Per-core	0, 1, 2, 3	Controls the number of wait states that are incurred by accesses to the ITCM. <m> is the core number.
ITCM_STRETCH_CLK<m>	Per-core	0, 1	ITCM RAMs clock pulse stretch. <m> is the core number.  <b>0</b> Not stretched <b>1</b> Stretched

Parameter name	Scope	Permitted values	Description
DTCM_SIZE<m>	Per-core	0, 16, 32, 64, 128, 256, 512, 1024	Controls the size of the <i>Data Tightly Coupled Memory</i> (DTCM). <m> is the core number.  0: DTCM logic is removed and RAM size is 0  16: 16KB cache  32: 32KB cache  64: 64KB cache  128: 128KB cache  256: 256KB cache  512: 512KB cache  1024: 1024KB cache
DTCM_WAIT<m>	Per-core	0, 1, 2, 3	Controls the number of wait states that are incurred by accesses to the DTCM. <m> is the core number.
DTCM_STRETCH_CLK<m>	Per-core	0, 1	DTCM RAMs clock pulse stretch. <m> is the core number.  <b>0</b> Not stretched <b>1</b> Stretched

### 1.3.2 Integration-time configuration options

The following table shows the integration-time configuration options that you can configure by setting the top-level inputs.



Note

In addition to the features in the following table, you can also configure the *Main Manager* (MM) and *Low-latency RAM* (LLRAM) broadcast signal behavior as defined by the AMBA® specification. See *Arm® Cortex®-R82AE Configuration and Integration Manual* for more information on the Cortex®-R82AE processor signals.

**Table 1-6: Integration-time configuration options**

Feature	Scope	Permitted values	Description
<i>Low-latency RAM</i> (LLRAM) manager interface	Global	0, 1	Implemented with CFGLLRAMIMP  <b>0</b> Not implemented. <b>1</b> Implemented.
LLRAM base address	Global	Any	Configured with CFGLLRAMBASEADDR[PA_W-1:28]
LLRAM enable out of reset	Global	0, 1	Configured with CFGLLRAMEN  <b>0</b> LLRAM disabled out of reset. <b>1</b> LLRAM enabled out of reset.

Feature	Scope	Permitted values	Description
LLRAM shared	Global	0, 1	Configured with CFGLLRAMSHARED.  If set to 1, it indicates that there are multiple clusters connected to the same LLRAM and share data across the cluster.  <b>0</b> LLRAM not shared.  <b>1</b> LLRAM shared.
Poison support for <i>Main Manager</i> (MM) port	Global	0, 1	Configured with CFGMMPOISON  <b>0</b> MM port does not support poison.  <b>1</b> MM port supports poison.
<i>Low-latency Peripheral Port</i> (LLPP) manager interface	Global	0, 1	Implemented with CFGLLPPIMP  <b>0</b> Not implemented. <b>1</b> Implemented.
LLPP base address	Global	Aligned to 128MB	Configured with CFGLLPPBASEADDR[PA_W-1:27]
<i>Shared Peripheral Port</i> (SPP) manager interface	Global	0, 1	Implemented with CFGSPPIMP  <b>0</b> Not implemented. <b>1</b> Implemented.
SPP base address	Global	Aligned to 128MB	Configured with CFGSPPBASEADDR[PA_W-1:27]
Base address of the TCMs on the <i>ACE-Lite Subordinate</i> (ACELS) interface	Global	Aligned to 16MB	Configured with CFGACELSTCMBASEADDR[PA_W-1:24]
Value of Multiprocessor Affinity Register affinity level 2	Global	-	Configured with CFGMPIDRAFF2[7:0]
Value of Multiprocessor Affinity Register affinity level 3	Global	-	Configured with CFGMPIDRAFF3[7:0]
GIC CPU interface disable	Global	0, 1	Configured with GICCDISABLE  <b>0</b> GIC CPU interface enabled. <b>1</b> GIC CPU interface disabled.
RAM protection enable out of reset	Global	0, 1	Configured with CFGGRAMPROTEN  <b>0</b> RAM protection disabled out of reset <b>1</b> RAM protection enabled out of reset
L2 cache POP EVA feature	Global	0, 1	Configured with CFGGL2EVAIMP  <b>0</b> L2 cache data RAMs do not implement the POP Eviction-Allocation optimization <b>1</b> L2 cache data RAMs implement the POP Eviction-Allocation optimization, and this is enabled out of reset

Feature	Scope	Permitted values	Description
Split/Hybrid/Lock mode select	Global	0b01, 0b10, 0b11	Selected with CFGCEMODE  <b>0b01</b> Split-mode (comparison logic inactive for both cores and cluster) <b>0b10</b> Hybrid-mode (comparison logic inactive for cores, active for cluster) <b>0b11</b> Lock-mode (comparison logic active for both cores and cluster)
ITCM base address	Per-core	Size-aligned to ITCM_SIZE<m>	Configured with CFGITCMBASEADDRm[PA_W-1:14] where m is the core number from 0 to NUM_CORES-1.
ITCM enable out of reset	Per-core	0, 1	Configured with CFGITCMENm where m is the core number from 0 to NUM_CORES-1.  <b>0</b> ITCM disabled out of reset. <b>1</b> ITCM enabled out of reset.
DTCM base address	Per-core	Size-aligned to DTCM_SIZE<m>	Configured with CFGDTCMBASEADDRm[PA_W-1:14] where m is the core number from 0 to NUM_CORES-1.
Data endianness	Per-core	0, 1	Configured with CFGENDm where m is the core number from 0 to NUM_CORES-1. Controls the out of reset value of the SCTLR_EL2.EE bit.  <b>0</b> Little-endian. <b>1</b> Byte-invariant big-endian.
Reset vector base address	Per-core	Aligned to 4B	Configured with CFGRVBARADDRm[PA_W-1:2] where m is the core number from 0 to NUM_CORES-1. Controls the out of reset value of the RVBAR_EL2.RVBARADDR field.

## 1.4 Supported standards and specifications

The Cortex®-R82AE processor complies with, or implements, the relevant Arm architectural standards and protocols, and relevant external standards.

This book complements architecture reference manuals, architecture specifications, protocol specifications, and relevant external standards. It does not duplicate information from these sources except for some system register content.

### Arm architecture

The Cortex®-R82AE processor implements the Arm®v8-R AArch64 architecture. This includes:

- AArch64 Execution state only. There is no support for AArch32 Execution state.
- Support for Exception levels EL0, EL1, and EL2. There is no support for EL3.
- A64 instruction set for the Arm®v8-R AArch64 architecture.
- Advanced SIMD and floating-point functionality that complies with ANSI/IEEE Std 754-2008, IEEE Standard for Binary Floating-Point Arithmetic.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

## Bus architecture

The Cortex®-R82AE processor is compliant with the following:

- AMBA 5 CHI (Issue E). See the [AMBA® CHI Architecture Specification](#).
- AMBA 5 AXI and ACE protocol (Issue H). See the [AMBA® AXI Protocol Specification](#).
- AMBA AXI5-Stream protocol (Issue B). See the [AMBA® AXI-Stream Protocol Specification](#).
- AMBA APB5 protocol (Issue D). See the [AMBA® APB Protocol Specification](#).
- AMBA ATB protocol (Issue C). See the [Arm® AMBA® 4 ATB Protocol Specification ATBv1.0 and ATBv1.1](#).

## Generic Interrupt Controller (GIC) architecture CPU interface

The Cortex®-R82AE processor supports the GICv3.2 architecture.

See the [Arm® Generic Interrupt Controller Architecture Specification, GIC architecture version 3 and version 4](#).

## Generic Timer architecture

The Cortex®-R82AE processor implements the Arm® Generic Timer architecture.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

## Debug architecture

The Cortex®-R82AE processor implements the Arm®v8-R AArch64 debug architecture including debug features up to Arm®v8.4 architecture, the Armv8.3-DoPD extension, and the Arm®v8.3 debug over powerdown support.

For more information, see the:

- [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).
- [Arm® CoreSight™ Architecture Specification v3.0](#).
- [Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual](#).

## Embedded Trace Macrocell (ETM) architecture

The Cortex®-R82AE processor implements the ETMv4.5 architecture.

See the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#) for more information.

## Performance Monitoring Unit (PMU)

The Cortex®-R82AE processor implements the PMUV3 architecture with the Arm®v8.4 PMU extension.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.



## Reliability, Availability, and Serviceability (RAS)

The Cortex®-R82AE processor implements the Arm®v8.4 RAS extension.

See the [Arm® Architecture Reference Manual Supplement Reliability, Availability, and Serviceability \(RAS\), for A-profile architecture](#) for more information.

## 1.5 Design process

The Cortex®-R82AE processor is delivered as a synthesizable RTL description in SystemVerilog *Hardware Description Language* (HDL). Before the Cortex®-R82AE processor can be used in a product, it must go through the following processes:

### Implementation

The implementer configures and synthesizes the RTL to produce a hard macrocell. This process includes integrating the cache, TCM, duplicate tag, and branch predictor RAMs into the design.

### Integration

The integrator connects the macrocell into a SoC. This process includes connecting the macrocell to a memory system and peripherals.

### Programming

In the final process, the system programmer develops the software to configure and initialize the Arm processor and tests the application software.

Each process can be performed by a different party. Implementation and integration choices affect the behavior and features of the Cortex®-R82AE processor.

The operation of the final device depends on the following:

### Build configuration

The implementer chooses the options that affect how the RTL source files are rendered. These options usually include or exclude logic that affects one or more of the area, maximum frequency, and features of the resulting macrocell.

### Configuration inputs

The integrator configures some features of the processor by tying inputs to specific values. These configuration settings affect the start-up behavior before any software configuration is made. They can also limit the options available to the software.

### Software configuration

The programmer configures the processor by programming particular values into registers. These configuration choices affect the behavior of the processor.

## 1.6 Documentation

The Cortex®-R82AE processor documentation describes the functionality of the processor and explains how to configure, integrate, and implement it.

The Cortex®-R82AE processor documentation includes a Technical Reference Manual, a Configuration and Integration Manual, and a Safety Manual.

### Technical Reference Manual

The *Technical Reference Manual* (TRM) describes the functionality and the key features of the processor. It is a helpful reference at all stages of the design flow. Some behavior described in the TRM might not be relevant because of the particular way that the Cortex®-R82AE processor is implemented and integrated. If you are programming the Cortex®-R82AE processor, you need additional information from:

- The implementer about the build configuration of the implementation.
- The integrator about the signal configuration of the device that you are using.

### Configuration and Integration Manual

The *Configuration and Integration Manual* (CIM) describes the Cortex®-R82AE processor deliverables and how to use them to perform implementation and integration of the processor.

The *Configuration and Integration Manual* (CIM) describes:

- How to configure the RTL source files with the build configuration options.
- How to integrate RAM arrays.
- How to validate the RTL.
- How to run delivered tests.
- Considerations for floorplanning.
- How to integrate the processor into a SoC. This includes describing the signals that must be tied off to configure the macrocell.
- The integration kit description.
- The processes to sign off the configured design.

If you are integrating an already-implemented macrocell of the Cortex®-R82AE processor you need additional information from the implementer about the build configuration of the implementation.

The Arm product deliverables include reference scripts and information on how to use them to implement your design. The methodology flows supplied by Arm are example reference implementations. For EDA tool support, contact your EDA vendor.

The CIM is a confidential manual that is available only to licensees.

## 1.7 Product revisions

The following product revisions have been released.

### **r0p0**

First beta release for r0p0

### **r0p0**

First early access release for r0p0

### **r0p1**

First release for r0p1

### **r0p1**

Second release for r0p1

## 2. Technical overview

This chapter describes the Cortex®-R82AE processor components and interfaces.

### 2.1 Terminology

In this manual, the following terms refer to the descriptions that are provided below.

#### Core

A core includes all the logic related to the data processing unit, memory system and management, power management, and core-level debug and trace logic. In the context of the Cortex®-R82AE processor, CPU and core are used interchangeably.

In this manual, NUM\_CORES refers to the number of cores within the Cortex®-R82AE processor and <m> refers to the core instance number.

#### Cluster

In the context of the Cortex®-R82AE processor, the cluster refers to the *CPU Bridge (System side)* (CBS), the *Shared Bridge* (SB), all cores, and the logic that is shared among cores. Shared logic includes the *CPU Bridge (CPU side)* (CBC), the L2 cache, and the coherency logic that maintains coherency between the caches in the cores and the L2 cache and the *Low-latency RAM* (LLRAM) memory. There is also shared debug logic at the cluster level.

#### Processor

In the context of the Cortex®-R82AE processor, the processor is the top-level unit that contains the cluster and the *Power Policy Units* (PPUs).

#### DebugBlock

DebugBlock is a dedicated debug component separate from the Cortex®-R82AE processor. The DebugBlock is instantiated as a separate top-level unit to allow you to implement the debug components in an always On power domain. Although instantiated as a separate unit, the DebugBlock still forms part of the Cortex®-R82AE processor.

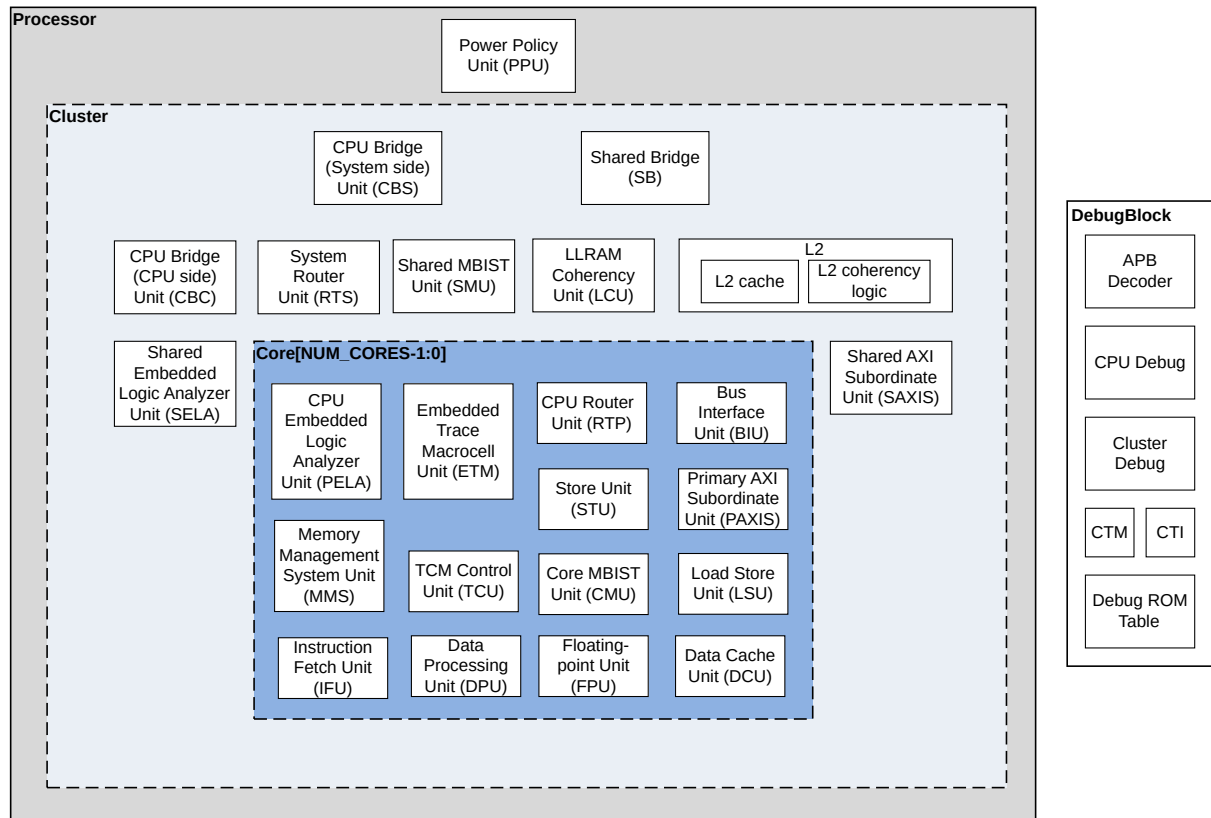
### 2.2 Components

The Cortex®-R82AE processor system includes two top-level modules:

- The Cortex®-R82AE processor
- The DebugBlock

The DebugBlock is separated from the Cortex®-R82AE processor to allow you to implement the debug components in an always On power mode, enabling debug over powerdown.

The following figure shows the main components of the Cortex®-R82AE processor.

**Figure 2-1: Functional block diagram**

## Power Policy Unit

The Cortex®-R82AE processor includes several *Power Policy Units* (PPUs) that control power modes and resets. The PPU can be programmed to directly select a specific power mode or to autonomously switch between power modes within a specified range, based on the requirements of the processor.

The PPU can be programmed using the Utility bus, either by a *System Control Processor* (SCP) or by the Cortex®-R82AE processor (through a loopback connection).

For more information on the PPUs, see [6. Power and reset control with PPUs](#) on page 97.

## Shared Bridge

The *Shared Bridge* (SB) decouples the DebugBlock and other components in the system from the CPU bridge in each core. The SB includes clock and power control logic for the cluster and interacts with the L2 coherency logic for SCLK clock gating.

## CPU Bridge (System side) Unit

There is one *CPU bridge (System side) Unit* (CBS) in the cluster. The CPU bridge controls buffering between the cores and the Cortex®-R82AE processor.

## CPU Bridge (CPU side) Unit

There is one *CPU Bridge (CPU side) Unit* (CBC) for all the cores in the cluster. The CPU bridge controls buffering between the cores and the Cortex®-R82AE processor.

## System Router Unit

The *System Router Unit* (RTS) is instantiated in the cluster as a single unit. The RTS controls the packet traffic at the cluster level such as routing the *Generic Interrupt Controller* (GIC) packets between the SB in the cluster and the *CPU Router Units* (RTPs) within the cores.

## Shared MBIST Unit

The *Shared MBIST Unit* (SMU) provides production and online MBIST for the *LLRAM Coherency Unit* (LCU) and L2 cache RAMs.

## LLRAM Coherency Unit

The *LLRAM Coherency Unit* (LCU) provides coherent access to the *Low-latency RAM* (LLRAM) port for up to eight cores. The LCU also provides coherent access to LLRAM port for an external agent that needs I/O coherency with the Cortex®-R82AE processor. The LCU also provides access to the *Shared Peripheral Port* (SPP).

## L2

The L2 consists of the L2 cache RAMs and the L2 coherency logic. The L2 is required to interface the cores to an AXI or a CHI interconnect.

For more information on the L2 memory system, see [8.4 L2 memory system](#) on page 138.

### L2 cache

The L2 cache is unified (it can cache both instructions and data) and shared by all the cores in the cluster. The L2 cache is 8-way, set-associative with a configurable size of 0KB, 128KB, 256KB, 512KB, 1MB, 2MB, or 4MB. Cache lines have a fixed length of 64 bytes.

### L2 coherency logic

The L2 coherency logic maintains coherency between all the cores and caches within the cluster for the *Main Manager* (MM) port accesses.

When the MM port is configured to be CHI and the cluster is connected to another coherent cluster through a coherent interconnect, the L2 coherency logic also automatically maintains coherency with that other cluster.

The L2 coherency logic contains buffers that can handle direct cache-to-cache transfers between cores without having to read or write data to the L2 cache. Cache line migration enables dirty cache lines to be moved between cores. There is no requirement to write back transferred cache line data to the L2 cache.

## Shared AXI Subordinate Unit

The *Shared AXI Subordinate Unit* (SAXIS) enables external read and write access to the *ACE-Lite Subordinate* (ACELS) port. These reads and writes are then routed to the *Primary AXI Subordinate Unit* (PAXIS) or the LCU.

## Shared Embedded Logic Analyzer Unit

The *Shared Embedded Logic Analyzer Unit* (SELA) provides support for a cluster level CoreSight™ ELA-600 *Embedded Logic Analyzer* to monitor the signals related to the shared logic.

## CPU Embedded Logic Analyzer Unit

The *CPU Embedded Logic Analyzer Unit* (PELA) provides support for per-core CoreSight™ ELA-600 to monitor the signals relate to the core. The configuration option to pre-integrate ELAs is global.



The CoreSight™ ELA-600 is a separately licensable product.

---

## Embedded Trace Macrocell Unit

Each core has an *Embedded Trace Macrocell* (ETM) unit that enables per-core ETM instruction and data trace on separate ATB buses:

- An ATB4 32-bit bus for instruction.
- An ATB4 128-bit bus for data and ELA.

The trace is generated per-core but the ATB buses are shared between the cores.

For more information on the ETM, see [15. ETM](#) on page 294.

## CPU Router Unit

There is one *CPU Router Unit* (RTP) that is instantiated within each core. The RTPs are connected to the RTS in the cluster.

Each RTP controls the packet traffic within the core such as routing packages between the RTP and the *Data Processing Unit* (DPU) in the core.

## Bus Interface Unit

The *Bus Interface Unit* (BIU) is responsible for driving the L2 and LCU read and write interfaces. The BIU receives the read and write requests from the *Load Store Unit* (LSU), *Data Cache Unit* (DCU), *Translation Lookaside Buffer* (TLB), *Instruction Fetch Unit* (IFU), and *Store Unit* (STU).

## Store Unit

The *Store Unit* (STU) merges and forwards (as appropriate) stores to *Instruction Tightly Coupled Memory* (ITCM), *Data Tightly Coupled Memory* (DTCM), L1 caches, *Low-latency Peripheral Port* (LLPP), *Shared Peripheral Port* (SPP), *Low-latency RAM* (LLRAM), and *Main Manager* (MM).

## Primary AXI Subordinate Unit

The *Primary AXI Subordinate Unit* (PAXIS) enables the read and write access to the *Tightly Coupled Memories* (TCMs). The reads and writes both directly route to the *TCM Unit* (TCU) from the PAXIS.

## Memory Management System Unit (MMS)

The Cortex®-R82AE processor implements *Protected Memory System Architecture* (PMSA) and optional *Virtual Memory System Architecture* (VMSA).

Hypervisor software running at EL2 selects between PMSA and VMSA on a per-operating system basis.

### Memory Protection Unit

The *Memory Protection Unit* (MPU) implements the PMSA and determines the attributes for each memory location including permissions, type, and cacheability. Two programmable MPUs are provided, controlled from EL1 and EL2 respectively.

Access permissions determine which levels of privilege are permitted to access a location and whether write access or instruction execution are permitted. Memory type and cacheability affect how the Cortex®-R82AE processor handles particular accesses, for example, if the processor permits two stores to be merged into a single write access. These attributes and their meanings are defined by the Arm architecture.

### Memory Management Unit

The *Memory Management Unit* (MMU) implements the VMSA and provides memory system control through a set of virtual-to-physical address mappings and memory attributes that are held in translation tables. This information is cached in the *Translation Lookaside Buffer* (TLB) when an address is translated. The TLB entries include global and *Address Space Identifiers* (ASIDs) to prevent context switch TLB flushes. They also include *Virtual Machine Identifiers* (VMIDs) to prevent TLB flushes on virtual machine switches by the hypervisor.

For more information on the memory management, see [9. Memory management](#) on page 216.

## TCM Control Unit

The *Tightly Coupled Memory Control Unit* (TCU) is responsible for arbitration between all requests to the *Instruction Tightly Coupled Memories* (ITCMs) and *Data Tightly Coupled Memories* (DTCMs). The TCU contains two arbitration pipelines for managing requests to ITCMs and DTCMs.

Each core within the Cortex®-R82AE processor has:

- An optional *Instruction Tightly Coupled Memory* (ITCM) with configurable size 0 or from 16KB to 1MB in powers of 2. ITCM provides lowest-latency access for instructions and data. Optional here means that the logic is always present but the size can be 0.



Note

ITCM is unified, that is, although it is optimized for instruction use, it is also available for data.

- 
- An optional *Data Tightly Coupled Memory* (DTCM) with configurable size 0 or from 16KB to 1MB in powers of 2. DTCM provides lowest-latency access for data only. Optional here means that the logic is always present but the size can be 0.





DTCM is for data only and it cannot be used to fetch instructions from.

---

For more information on the TCMs, see [8.2 TCM memories](#) on page 124.

### Core MBIST Unit

The *Core MBIST Unit* (CMU) provides production and online MBIST for the core RAMs.

### Load Store Unit

The *Load Store Unit* (LSU) is responsible for execution of all instructions that affect the L1 data memory system.

### Instruction Fetch Unit

The *Instruction Fetch Unit* (IFU) speculatively fetches instructions from the *Instruction Tightly Coupled Memory* (ITCM), L1 instruction cache, or the main memory.

The IFU predicts the outcome of branches in the instruction stream and passes the instructions to the *Data Processing Unit* (DPU) for processing.

### Data Processing Unit

The *Data Processing Unit* (DPU) includes the instruction decoders, the integer execution pipelines, and the control logic of the Cortex®-R82AE processor. It receives instructions from the IFU. The DPU executes the integer instructions and works in conjunction with the FPU and LSU to execute FP/SIMD instructions and instructions which require data transfer to or from the memory system.

The DPU interfaces with IFU, LSU, STU, DCU, TCU, LCU, RTP, ETM, and CBC.

The DPU implements the *Generic Interrupt Controller* (GIC) CPU interface as well as the *Performance Monitoring Unit* (PMU).

### Floating-point Unit

The *Floating-point Unit* (FPU) is responsible for decoding and executing the Advanced SIMD and floating-point instructions.

Supporting Advanced SIMD and floating-point instructions is optional and can be configured separately per-core by the `NEON_FP` parameter.

Advanced SIMD is a media and signal processing architecture that adds instructions primarily for audio, video, 3D graphics, image, and speech processing. The floating-point architecture provides support for half-precision, single-precision, and double-precision floating-point operations.

**Note**

The Advanced SIMD architecture, its associated implementations, and supporting software, are also referred to as Arm® Neon™ technology.

For more information on the Advanced SIMD and floating-point support, see [16. Advanced SIMD and floating-point support](#) on page 305.

## Data Cache Unit

The *Data Cache Unit* (DCU) is responsible for all operations accessing the L1 Data cache. The DCU arbitrates between the requests and is responsible for responding to snoop requests to maintain coherency.

## DebugBlock

The DebugBlock transfers trigger events to/from the Cortex®-R82AE processor.

The DebugBlock is separated from the Cortex®-R82AE processor to facilitate the following system design options:

- The DebugBlock is placed in a separate power domain, to ensure that it is possible to maintain the connection to a debugger while the cores and cluster are powered down.
- The DebugBlock is physically placed with the other CoreSight logic in the SoC, rather than close to the cluster.

The separate power domains allow the cores and the cluster to be powered down while maintaining essential state that is required to continue debugging. Separating the logical power domains into physical domains is optional and might not be available in individual systems.

## APB Decoder

The APB Decoder is responsible for gathering the external CoreSight component signals such as *Debug Access Port* (DAP) inputs and the debug events from the Cortex®-R82AE processor. It then generates the internal select signals to activate the appropriate internal component within the DebugBlock.

## CPU Debug

The CPU Debug handles all core related accesses from both the external CoreSight component and the Cortex®-R82AE processor and generates all the necessary transactions to a core within the Cortex®-R82AE processor.

There is one CPU Debug module for each core within the Cortex®-R82AE processor.

## Cluster Debug

The Cluster Debug handles all cluster related accesses from both the external CoreSight component and the Cortex®-R82AE processor and generates all the necessary transactions to relevant cluster components such as the cluster PMU and cluster ELA.

There is one Cluster Debug module for all the cluster components.

## CTI and CTM

The DebugBlock implements *Embedded Cross Trigger* (ECT). A *Cross Trigger Interface* (CTI) is allocated to each core within the Cortex®-R82AE processor. An additional CTI is allocated to the cluster PMU and, if present, to the cluster ELA.

The CTIs enable the debug logic, ETM, and other CoreSight components to interact with each other.

The CTIs are interconnected through the *Cross Trigger Matrix* (CTM). A single external channel interface is implemented to allow cross-triggering to be extended to the SoC.

## Debug ROM Table

The Debug ROM table contains a list of components in the system. Debuggers can use the Debug ROM table to determine which CoreSight components are implemented.

## 2.3 Interfaces

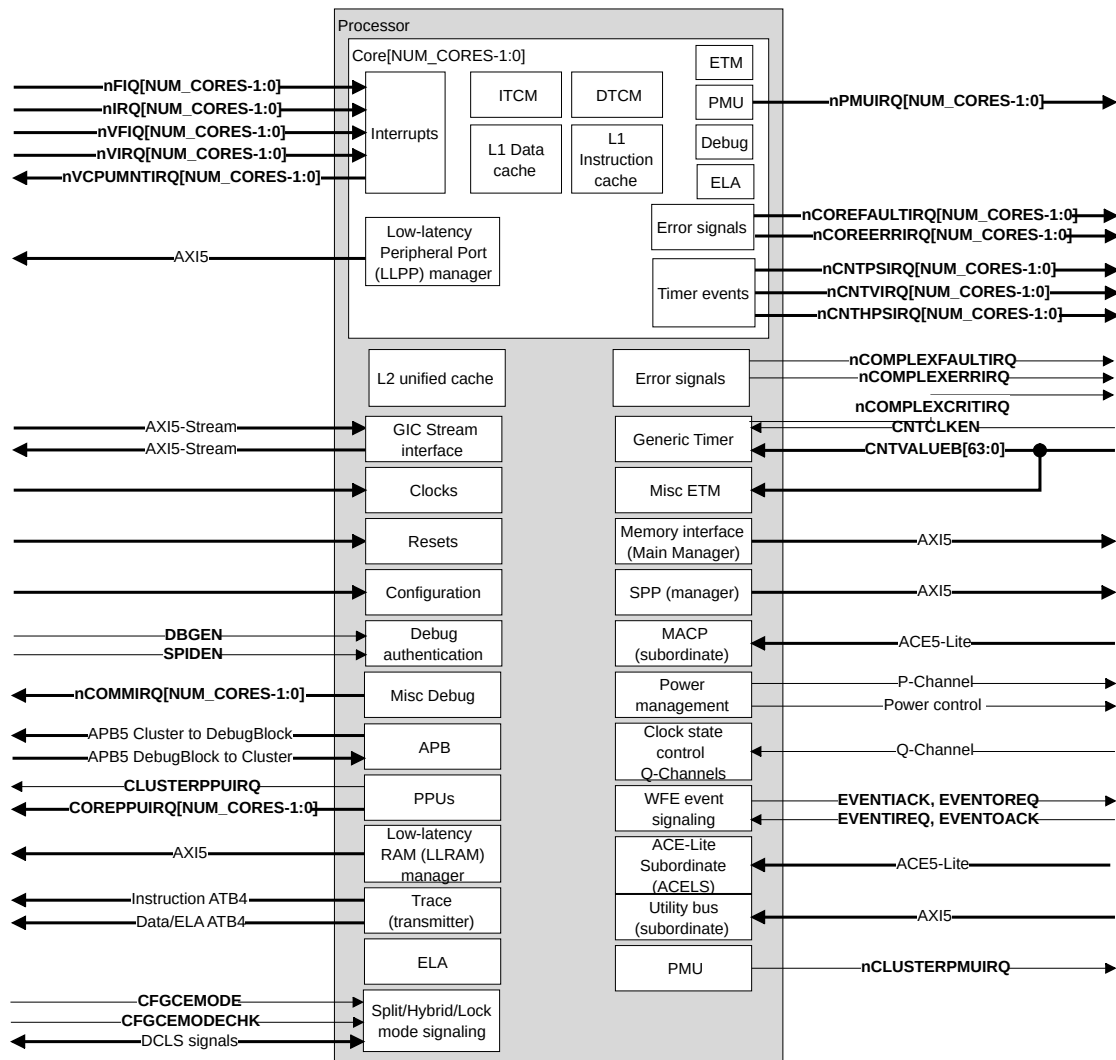
The Cortex®-R82AE processor has several interfaces to connect it to a SoC.

The following figure shows the interfaces of the Cortex®-R82AE processor.



NUM\_CORES is the number of physical cores. See [1.3.1 Configuration parameters](#) on page 27 for permitted values.

---

**Figure 2-2: Processor interfaces**

The following table describes the interfaces of the Cortex®-R82AE processor.

**Table 2-1: Processor interfaces**

Purpose	Protocol	Notes
Low-latency Peripheral Port (LLPP)	AMBA® AXI5 (Issue H) 32-bit	Each core within the Cortex®-R82AE processor has an optional private LLPP manager for minimum latency access to memory and devices outside the cluster.

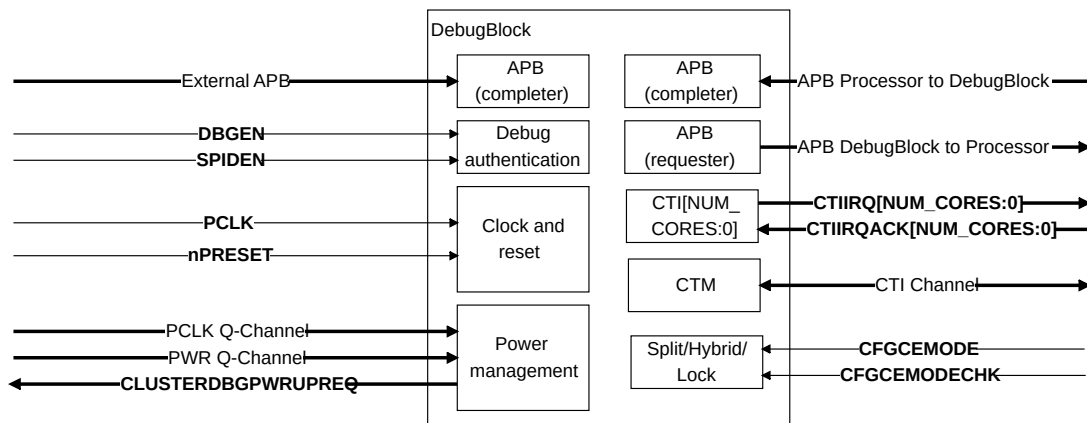
Purpose	Protocol	Notes
Generic Interrupt Controller (GIC) Stream interface (processor to GIC)	AMBA® AXI5-Stream (Issue B) 32-bit	AXI5-Stream interface for interrupts from the Cortex®-R82AE processor to the GIC.
GIC Stream interface (GIC to processor)	AMBA® AXI5-Stream (Issue B) 32-bit	AXI5-Stream interface for interrupts from the GIC to the Cortex®-R82AE processor.
Cortex®-R82AE processor to DebugBlock	AMBA® APB5 (Issue D) 32-bit	APB interface from the Cortex®-R82AE processor to the DebugBlock.
DebugBlock to Cortex®-R82AE processor	AMBA® APB5 (Issue D) 32-bit	APB interface from the DebugBlock to the Cortex®-R82AE processor.
Low-latency RAM (LLRAM)	AMBA® AXI5 (Issue H) 256-bit	The Cortex®-R82AE processor has an optional LLRAM for low latency access to memory shared between cores within the cluster.
Trace	AMBA® ATB4 (Issue C) 32-bit instruction ATB trace  128-bit data ATB trace	The Cortex®-R82AE processor has two transmitter ATB interfaces for instructions and data. An instruction trace funnel funnels all the processor ETM instruction trace streams into a single ATB trace bus. A data trace funnel funnels all the processor ETM data trace streams and all the ELA trace streams into a single ATB trace bus.
DCLS and CEMODE signaling signaling	-	Includes: <ul style="list-style-type: none"> <li>Split/Hybrid/Lock mode select inputs</li> <li>Control inputs and reporting outputs</li> </ul>
Utility bus	AMBA® AXI5 (Issue H) 64-bit	The Cortex®-R82AE processor has a subordinate Utility bus that manages power states and provides access to <i>Power Policy Units</i> (PPUs) registers, <i>Reliability, Availability, and Serviceability</i> (RAS) registers, and PMC registers in each core and the cluster.
ACE-Lite Subordinate (ACELS)	AMBA® ACE5-Lite (Issue H) 128-bit	The Cortex®-R82AE processor has a subordinate ACELS bus that enables external agents to access to the TCMs and LLRAM port.
WFE event signaling	-	Signals for <i>Wait For Event</i> (WFE) wake-up events.
Clock state control	Q-Channel	Q-Channels for clock gating control.
Power state control	P-Channel	P-Channels for Cortex®-R82AE processor power management.
Main Accelerator Coherency Port (MACP)	AMBA® ACE5-Lite (Issue H) 128-bit	The Cortex®-R82AE processor has a subordinate MACP that provides access to the MM port to external managers.
Shared Peripheral Port (SPP)	AMBA® AXI5 (Issue H) 64-bit	The Cortex®-R82AE processor has an optional shared SPP manager for minimum latency access to memory and devices.

Purpose	Protocol	Notes
Main Manager (MM)	AMBA® AXI5 (Issue H) or AMBA® CHI (Issue E)	The Cortex®-R82AE processor has a configurable shared MM port for accesses to high-latency memory and non-critical peripherals.
Power management	P-Channel and Q-Channel	Cortex®-R82AE enables communication to an external power controller for clock gating and powerdown.
Generic Timer	-	Input for the Generic Timer counter value. The counter value is distributed to all cores. Each core outputs timer events.
Design for Test (DFT)	-	Interface to support access for <i>Automatic Test Pattern Generation</i> (ATPG) scan-path testing.

## DebugBlock interfaces

The following figure shows the interfaces of the DebugBlock.

**Figure 2-4: DebugBlock interfaces**



The following table describes the external interfaces of the DebugBlock.

**Table 2-2: DebugBlock interfaces**

Purpose	Protocol	Notes
External APB	AMBA® APB5 (Issue D)	Completer interface to external debug component, for example a <i>Debug Access Port</i> (DAP). Allows access to Debug registers and resources.
Cortex®-R82AE processor to DebugBlock	AMBA® APB5 (Issue D)	APB interface from the Cortex®-R82AE processor to the DebugBlock.
DebugBlock to Cortex®-R82AE processor	AMBA® APB5 (Issue D)	APB interface from the DebugBlock to the Cortex®-R82AE processor.
Cross-trigger channel interface	CTI	Allows cross-triggering to be extended to external SoC components.
Split/Hybrid/Lock	-	Split/Hybrid/Lock mode select input

Purpose	Protocol	Notes
Power management	Q-Channel	Enables communication to an external power controller to control clock gating and powerdown.

## 2.4 Functional safety and reliability

The following are the Cortex®-R82AE processor functional safety and reliability features.

- The Cortex®-R82AE processor implements memory protection logic for its internal memories. The processor is capable of detecting all 1-bit and 2-bit errors, and is capable of correcting at least all 1-bit errors. This is achieved through a variety of *Error Correcting Codes* (ECC) (either SECDED or DED) and exploiting non-RAM based redundancy. The TCMs, L1 I-Cache, L1 D-Cache, TLB, L2 Cache, L2 Data Buffer and L2/LCU Duplicate L1 Tag RAMs are all protected. All ECC errors are reported via the *Reliability, Availability, and Serviceability* (RAS) Extension support.
- Optional bus protection, implemented as odd parity, for all interfaces that are active during mission mode. This includes the Main Manager, *Low Latency RAM* (LLRAM), *Shared Peripheral Port* (SPP), *Low Latency Peripheral Port* (LLPP), *Main ACP* (MACP) and *ACE5-Lite Subordinate* (ACELS) memory system interfaces, as well as the *Utility Bus* (UB) for external system register accesses. In addition all mission-mode configuration signals, interrupt signals and power signaling is protected.
- *Dual-Core Lock-Step* (DCLS) operation is supported. In DCLS configurations, there is a second, redundant copy of the majority of the processor core and *Internal Wakeup Interrupt Controller* (IWIC) logic. Primary and redundant clock and reset pins are included on the Cortex®-R82AE processor and connected to the primary and secondary copies of the logic respectively. All functional inputs to the logic are duplicated and connected to both copies of the logic. The outputs from the two copies of logic are compared for errors. Faults can occur in either copy of the logic and cause errors on the outputs, however, comparators cannot determine whether the primary or redundant copy of DCLS faults will be indicated via dedicated top-level fault outputs.
- Optional *Programmable MBIST Controller* (PMC-100) for embedded memory and ECC logic testing during processor run-time. For more information, see the *Arm® PMC-100 Technical Reference Manual*. The processor also supports direct access to the PMC-100 from an external agent in the system through the Utility Bus. Access to the PMC-100 on this interface is only permitted for requests marked as secure and privileged in TUSER for Utility Bus.
- Optional licensable *Software Test Library* (STL), which is designed to provide high diagnostic fault coverage in a compact code image with short runtime. The Cortex®-R82AE processor includes an SBIST controller and supporting logic to increase testability and observability of faults in order to facilitate STL testing.
- Optional Bus Protection capability to protect against faults which may occur in the connection between the Cortex®-R82AE processor external interfaces and the connection to a safe-interconnect or endpoint. Bus Protection will follow the AMBA standard for all AMBA interfaces, and follow an odd parity scheme for all functional interfaces otherwise. Interfaces which are not active during mission mode, for example debug/trace, are excluded from bus protection and are not protected. A RAS event will be generated whenever a bus protection error occurs.

- Optional Flop Parity in order to protect against transient faults in the logic, primarily for use in systems where LOCK DCLS mode is not used. Flop parity adds parity checking for groups of common-enabled registers in the design. Parity is calculated on the inputs to the groups of registers and the parity bit is captured in an additional register. The output of the group of registers is used to recalculate the parity bit and compare it against the captured parity bit in order to detect transient faults in the register. Flop parity errors will be indicated through dedicated top level fault outputs and a RAS event.
- Optional address folding in order to incorporate address bits alongside data when generating and checking ECC codes. Address folding provides some protection against address decoder and related faults in the RAM. This is achieved by generating an ECC error if a read access is routed to the wrong RAM location due to a fault inside the RAM.
- A bus timeout feature designed to detect when a response is not received on an external interface within a customer-defined limit, based on the system design. This timeout mechanism can be used to trigger an exception if the bound is reached and the pipeline is stalled waiting for a response, allowing the fault to be handled. Bus timeout is supported on the MM, LLRAM, SPP and LLPP interfaces. A RAS event will be generated whenever a bus timeout error occurs.
- A per-core interrupt monitor for detecting the following scenarios:
  - If the core has been executing with interrupts masked for more than a programmable number of cycles
  - If the core has been pending in a WFI/WFE state but has not received a wakeup interrupt/event within a programmable number of cycles
  - A RAS event will be generated when the interrupt monitor detects an issue
- A livelock detector which will detect when a core has taken the same exception 10 times without retiring any other instructions. This may typically occur as a result of hard errors in the RAMs (for example, errors for which a write cannot remove the error) beyond the capacity of the Cortex®-R82AE processor to guarantee forward progress. A RAS event will be generated when this scenario occurs.
- Dedicated per-core SERR Interrupt input pins to allow external error events to interrupt a Cortex®-R82AE core, for example, as a result of a system error condition which needs handling
- Cortex®-R82AE supports the ARM GICv3.2 architecture and implements a pair of 32-bit AXI5-Stream interfaces to connect to an external GICv3.2 compliant distributor. Cortex®-R82AE is optimized for low interrupt latency when using low latency SPIs with an appropriate low latency GICv3.2 compliant GIC such as GIC-Fainlight.



## 3. Programmers' model

This chapter provides a brief description of the Arm®v8-R AArch64 architecture for programmers.

For a complete description of the programmers' model, refer to the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

### 3.1 About the programmers' model

The Cortex®-R82AE processor implements the Arm®v8-R AArch64 architecture. This includes:

- AArch64 Execution state only. There is no support for AArch32 Execution state.
- Support for Exception levels EL0, EL1, and EL2. There is no support for EL3.
- Secure state operation only at all Exception levels using the Secure-EL2 security model. There is no support for Non-secure state at any EL.
- Full implementation of the Arm®v8-A A64 instruction set with Arm®v8-R AArch64 *Instruction Set Architecture* (ISA) extensions.
- *Protected Memory System Architecture* (PMSA) at EL1 and EL2.
- *Optional Virtual Memory System Architecture* (VMSA) only at EL1.
- Arm®v8-R AArch64 debug architecture including debug features up to Arm®v8.4 architecture and the debug over powerdown support.
- *Generic Interrupt Controller* (GIC) with the GICv3.2 architecture.
- Advanced SIMD and floating-point operations in the A64 instruction set.

### 3.2 Arm®v8-R AArch64 architecture concepts

The following sections provide an introduction to the main architectural concepts and terminology used throughout the rest of this document.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.



An understanding of the terminology defined in this section is a prerequisite for understanding the remainder of this manual.

---

### 3.2.1 Architecture requirements

The Cortex®-R82AE processor supports all the mandatory features from the Arm®v8.4 architecture and some optional features from the Arm®v8.5 and Armv8.6 architectural extensions.

The following table shows the architectural features that are implemented by the Cortex®-R82AE processor.

**Table 3-1: Architectural features implemented by the processor**

FEAT_GICv3	Generic Interrupt Controller v3	Yes
FEAT_GICv3p1	Generic Interrupt Controller v3.1	Yes
FEAT_GICv3_NMI	Non-maskable interrupts	No
FEAT_GICv3_LEGACY	Support for GICv2 legacy operation	No
FEAT_GICv3_TDIR	Trapping EL1 writes to ICV_DIR	Yes
FEAT_GICv4	Generic Interrupt Controller v4	No
FEAT_GICv4p1	Generic Interrupt Controller v4.1	No
FEAT_PMUv3	PMU extension	Yes
FEAT_ETMv4	Embedded Trace Macrocell v4.0	Yes
FEAT_ETMv4p1	Embedded Trace Macrocell v4.1	Yes
FEAT_ETMv4p2	Embedded Trace Macrocell v4.2	Yes
FEAT_ETMv4p3	Embedded Trace Macrocell v4.3	Yes
FEAT_ETMv4p4	Embedded Trace Macrocell v4.4	Yes
FEAT_ETMv4p5	Embedded Trace Macrocell v4.5	Yes
FEAT_ETMv4p6	Embedded Trace Macrocell v4.6	No
FEAT_RAS	Reliability, Availability and Serviceability extension	Yes
FEAT_SPE	Statistical Profiling Extension	No
FEAT_SVE	Scalable Vector Extension	No
FEAT_AMUv1	Activity Monitors	No
FEAT_MPAM	Memory Partitioning and Monitoring	No
FEAT_PCSRv8	PC Sample-based Profiling extension	Yes
FEAT_SHA1	SHA1 and SHA2-256 functionality	No
FEAT_SHA256		
FEAT_AES	Advanced Encryption Standard	No
FEAT_PMULL		
FEAT_DoubleLock	Double Lock	No
FEAT_SSBS	Speculative Store Bypass Safe	Yes
FEAT_SSBS2		
FEAT_CSV2	Cache Speculation Variant 2: Implementation of CSV2 without SCXTNUM registers	Yes
FEAT_CSV2_1p1		Yes
FEAT_CSV2_1p2		No
FEAT_CSV2_2		No

FEAT_CSV3	Cache Speculation Variant 3	Yes
FEAT_SB	Speculation Barrier	Yes
FEAT_SPECRES	Prediction Invalidation	Yes
FEAT_CP15SDISABLE2	Prevents writes to a set of Secure CP15 registers	No
-- (dropped)	Floating Point Extensions	Yes, when NEON_FPm == 1
-- (dropped)	Advanced SIMD Extensions	Yes, when NEON_FPm == 1
FEAT_DGH	Data Gathering Hint	Yes
FEAT_ETS	Enhanced Translation Synchronization	No
FEAT_nTLBPA	Intermediate caching of translation table walks	Yes (nTLBPA set to 1)
FEAT_CRC32	CRC32 Instructions	Yes
FEAT_LSE	Large System Extensions	Yes
FEAT_RDM	Rounding Double Multiply Accumulate	Yes, when NEON_FPm == 1
FEAT_HPDS	Hierarchical Permission Disables	Yes, when VMSAm == 1
FEAT_VHE	Virtualization Host Extensions	No
FEAT_PAN	Privileged Access-Never	Yes
FEAT_PAN3	Support for SCTLr_ELx.EPAN	No
FEAT_LOR	Limited Ordering Regions	No
FEAT_HAFDBS	Translation Table Hardware Management	Yes, when VMSAm == 1
FEAT_VMID16	16-bit VMID	No
FEAT_PMUv3p1	Arm v8.1 PMU extensions	Yes
--- (dropped)	Arm v8 debug with VHE	No
FEAT_TTCNP	Translation Table Common Not Private translations	Yes, when VMSAm == 1
FEAT_XNX	Translation Table Stage 2 Unprivileged Execute-Never	Yes
FEAT_UAO	PSTATE override of Unprivileged Load/Store	Yes
FEAT_PAN2	AT S1E1R and AT S1E1W instruction variants	Yes
FEAT_DPB	Data Cache clean to Point of Persistence	Yes
FEAT_Debugv8p2	Arm v8.2 Debug extensions	Yes
FEAT_ASMv8p2	Arm v8.2 changes to the A64 Instruction Set Architecture	Yes
FEAT_IESB	Implicit Error Synchronization Barrier	Yes
FEAT_AA32HPD	AArch32 Hierarchical Permission Disables	No
FEAT_HPDS2	Translation Table Page Based Hardware Attributes	No
FEAT_LSMAOC	Load/Store Multiple Atomicity and Ordering Controls	No
FEAT_FP16	Half-precision floating-point data processing	Yes, when NEON_FPm == 1
FEAT_LVA	Large VA support	No
FEAT_LPA	Large PA and IPA support	No

FEAT_VPIPT	VMID-aware PIPT instruction cache	No
FEAT_PCSRv8p2	Arm v8.2 PC Sample-based Profiling extension	Yes
FEAT_DotProd	Dot Product instructions	Yes, when NEON_FPm == 1
FEAT_FHM	Floating-point Half-precision Multiplication instructions	Yes, when NEON_FPm == 1
FEAT_SHA512	Cryptography support for SHA512 and SHA3 instructions	No
FEAT_SHA3		
FEAT_SM3	Cryptography support for SM instructions	No
FEAT_SM4		
FEAT_EVT	Enhanced Virtualization Traps	No
FEAT_DPB2	Cache Clean to Point of Deep Persistence	Yes
FEAT_BF16	BFloat16 extension	No
FEAT_AA32BF16	AArch32 BFloat16 extension	No
FEAT_I8MM	Int8 Matrix Multiplication	No
FEAT_AA32I8MM	AArch32 Int8 Matrix Multiplication	No
FEAT_F32MM	Single-precision Matrix Multiplication	No
FEAT_F64MM	Double-precision Matrix Multiplication	No
FEAT_PAuth	Pointer Authentication	Yes
FEAT_EPAC	Enhanced Pointer authentication	No
FEAT_PACQARMA5	Pointer authentication - QARMA5 algorithm	No
FEAT_PACIMP	Pointer authentication - IMPLEMENTATION DEFINED algorithm	No
FEAT_PACQARMA3	Pointer authentication - QARMA3 algorithm	Yes
FEAT_PAuth2	Enhancements to pointer authentication	Yes
FEAT_FPAC	Faulting on AUT* instructions	Yes
FEAT_FPACCOMBINE	Combined pointer authentication instructions	Yes
FEAT_CONSTPACFIELD	PAC algorithm enhancement	Yes
FEAT_JSCVT	JavaScript Conversion instruction	Yes, when NEON_FPm == 1
FEAT_NV	Nested Virtualization	No
FEAT_LRCPC	Weaker release consistency	Yes
FEAT_FCMA	Floating-point Complex Number support	Yes, when NEON_FPm == 1
FEAT_CCIDX	Cache extended number of sets	No
FEAT_SPEv1p1	Arm v8.3 Statistical Profiling Extensions	No
FEAT_DoPD	Arm v8.3 Debug over Power-Down	Yes
FEAT_SEL2	Secure EL2	Yes
FEAT_NV2	Enhanced support for Nested Virtualization	No
FEAT_S2FWB	Stage 2 Forced Write-Back	Yes
FEAT_DIT	Data Independent Timing	Yes
FEAT_IDST	ID Space Trap handling	Yes

FEAT_FlagM	Arm v8.4 Condition flag Manipulation	Yes
FEAT_LSE2	Arm v8.4 Large System Extensions	Yes
FEAT_LRCPC2	Arm v8.4 enhancements to weaker release consistency	Yes
FEAT_TLBIOS	TLB maintenance and TLB range instructions	Yes
FEAT_TLBIRANGE		
FEAT_TTL	Translation Table Level	Yes, when $VMSAm == 1$
FEAT_BBM	Change in size of page table mappings	Yes, when $VMSAm == 1$
FEAT_CNTSC	Generic Counter Scaling	Yes
FEAT_RASv1p1	RAS extensions for Arm v8.4	Yes
FEAT_DoubleFault	Double Fault Extension	No
FEAT_Debugv8p4	Arm v8.4 Debug relaxations and extensions	Yes
FEAT_PMUV3p4	Arm v8.4 PMU extensions	Yes
FEAT_TRF	Arm v8.4 Self-hosted Trace extensions	Yes
FEAT_TTST	Small translation tables	Yes, when $VMSAm == 1$
FEAT_FlagM2	Arm v8.5 Condition flag Manipulation	No
FEAT_FRINTTS	Floating-point to integer	No
FEAT_ExS	Context synchronization and exception handling	No
FEAT_GTG	Guest Translation Granule size	No
FEAT_BTI	Branch Target Identification	No
FEAT_EOPD	Preventing ELO access to halves of the address map	Yes, when $VMSAm == 1$
-- (decided it's Not a feature)	Prefetch speculation protection (Concurrent Modification Execution)	Yes
FEAT_RNG	Random Number Generator	No
FEAT_MTE	Memory Tagging extension	No
FEAT_MTE2		
FEAT_MTE3	MTE Asymmetric Fault Handling	No
FEAT_PMUV3p5	Arm v8.5 PMU extensions	No
FEAT_RNG_TRAP	Trapping support for RNDR/RNDRRS	No
FEAT_ECV	Enhanced Counter Virtualization	No
FEAT_FGT	Fine-Grained Traps	No
FEAT_TWED	Trapping of WFE	No
FEAT_AMUv1p1	Armv8.6 AMU extensions	No
FEAT_MPAMv0p1	Arm v8.6 MPAM extension	No
FEAT_MPAMv1p1		
FEAT_MTPMU	Multi-threaded PMU extensions	No
FEAT_AFP	Alternate floating-point behavior	No
FEAT_RPRES	Increased precision of Reciprocal Estimate and Reciprocal Square Root Estimate	No
FEAT_LS64	Support for 64 byte loads/stores	No

FEAT_LS64_V		
FEAT_LS64_ACCDATA		
FEAT_WFxT	WFE and WFI instructions with timeout	No
FEAT_HCX	Support for the HCRX_EL2 register	No
FEAT_LPA2	Larger physical address for 4KB and 16KB translation granules	No
FEAT_XS	XS attribute	No
FEAT_PMUV3p7	Armv8.7 PMU extensions	No
FEAT_SPEv1p2	Armv8.7 SPE features	No
FEAT_MOPS	Standardization of memory operations	No
FEAT_HBC	Hinted conditional branches	No
FEAT_NMI	Non-maskable Interrupts	No
FEAT_TIDCP1	ELO use of IMPLEMENTATION DEFINED functionality	No
FEAT_CMOW	Control for cache maintenance permission	No
FEAT_PMUV3p8	Armv8.8 PMU extensions	No
FEAT_HPMN0	Setting of MDCR_EL2.HPMN to zero	No
FEAT_PMUV3_TH	Event counting threshold	No
FEAT_SPEv1p3	Armv8.8 Statistical Profiling Extensions	No
FEAT_Debugv8p8	Debug v8.8	No

### 3.2.2 Execution state

The Arm®v8-R AArch64 architecture has only one Execution state, AArch64.

The Execution state defines the processor execution environment, including:

- Supported register widths.
- Supported instruction sets.
- Significant aspects of:
  - The execution model.
  - *Protected Memory System Architecture* (PMSA).
  - *Virtual Memory System Architecture* (VMSA).
  - The programmers' model.

### 3.2.3 Exception levels

In the Arm®v8-R AArch64 architecture, execution occurs at one of three Exception levels, ELO, EL1, and EL2. The Exception level determines the level of privilege where:

- ELO has the lowest software execution privilege. Execution at ELO is called unprivileged execution.

- Moves to a higher Exception level, such as from EL0 to EL1, indicate increased software execution privilege.
- EL2 provides support for processor virtualization.

The architecture does not specify what software runs at each Exception level, and such choices are outside the scope of the architecture. However, the following is a common usage model for the Exception levels:

<b>EL0</b>	Application.
<b>EL1</b>	Operating System.
<b>EL2</b>	Hypervisor.



Note

Unlike AArch32, the AArch64 execution state does not sub-divide any of the Exception levels into different modes.

### Changing Exception levels

When an exception is taken, the processor changes to the Exception level that supports the handling of the exception.

<b>Taking an exception</b>	An exception is <i>generated</i> when the processor first responds to an exceptional condition. The processor state at this time is the state the exception is <i>taken from</i> . The processor state immediately after taking the exception is the state the exception is <i>taken to</i> .
<b>Returning from an exception</b>	To return from an exception, the processor must execute an exception return instruction. The processor state when an exception return instruction is committed for execution is the state the exception <i>returns from</i> . The processor state immediately after the execution of that instruction is the state the exception <i>returns to</i> .

Execution can move between different Exception levels only on taking an exception, or on returning from an exception. Movement between Exception levels follows these rules:

- On taking an exception, the Exception level either increases or remains the same. An exception cannot be taken to a lower Exception level.
- On returning from an exception, the Exception level either decreases or remains the same. An exception cannot return to a higher Exception level.
- There is no exception handling at level EL0. Exceptions must be handled at a higher Exception level.

The Exception level that execution changes to or remains in, on taking an exception, is called the *target* Exception level of the exception, and:

- Every exception type has a target Exception level that is either:
  - Implicit in the nature of the exception.
  - Defined by configuration bits in the system registers.

- An exception cannot target EL0.

### 3.2.4 Instruction set architecture

The Arm®v8-R AArch64 architecture supports the A64 instruction set with Arm®v8-R AArch64 *Instruction Set Architecture* (ISA) extensions.

Arm®v8-R AArch64 ISA extensions add the following modifications to the original A64 ISA.

**Table 3-2: Arm®v8-R AArch64 ISA extensions**

Instructions	Change from A64
DFB	New instruction
DSB	Redefined
DMB	Redefined
DCPS3	Not supported
SMC	Not supported

The A64 instruction set provides access to 64-bit wide integer registers and data operations. Instruction opcodes, however, are still 32-bit long, not 64-bit long.

The Arm®v8-R AArch64 architecture does not support the A32 or T32 instruction sets.

### 3.2.5 Data types

The Arm®v8-R AArch64 architecture supports the following integer data types:

- Byte (8 bits).
- Halfword (16 bits).
- Word (32 bits).
- Doubleword (64 bits).

The Arm®v8-R AArch64 architecture also supports half-precision, single-precision, and double-precision floating-point data types as well as 64-bit and 128-bit wide vectors.

### 3.2.6 Arm®v8-R AArch64 registers

The Arm®v8-R AArch64 architecture has the following registers.

#### General-purpose registers

The Arm®v8-R AArch64 architecture provides thirty-one 64-bit general-purpose registers for instruction processing. General-purpose registers are accessible at all times and at all Exception levels. Each register can be accessed as:

- A 64-bit general-purpose register named X0 to X30.



- A 32-bit general-purpose register named W0 to W30.

The X30 general-purpose register is used as the procedure call link register.

In addition to the thirty-one general-purpose registers, there are also following special registers:

- Three 64-bit dedicated *Stack Pointer* (SP) registers for Exception levels EL0, EL1, and EL2.
- A 64-bit *Program Counter* (PC) holding the address of the current instruction. Software cannot write directly to the PC.
- Two *Exception Link Registers* (ELR) holding the exception return address for Exception levels EL1 and EL2.
- Two *Saved Program Status Registers* (SPSR) holding the state on taking exceptions for Exception levels EL1 and EL2.
- If the Cortex®-R82AE processor is configured with Neon™ technology, thirty-two 128-bit Advanced SIMD and floating-point registers. These registers can be accessed as 32-bit registers S0-S31, or as 64-bit registers D0-D31, or as 128-bit registers Q0-Q31, but these are different views of the same data.

## Process state, PSTATE

Process state or PSTATE is an abstraction of process state information. PSTATE holds information including:

- Flags that can be set by certain instructions and that determine the behavior of other instructions.
- Status bits that reflect the current Exception level and other states of the processor.
- Control bits that determine, for example, interrupt masking and data endianness.

## System registers

System registers provide system control or status reporting. For example, a register might provide syndrome information about an abort exception that the core has taken, or provide a control to enable or disable a cache.

The System registers use a standard naming format, <register\_name>.<bit\_field\_name>, to identify specific registers and the control and status bits within a register. Bits can also be described by their numerical position in the form <register\_name>[x:y] or the generic form bits[x:y].

The System registers include:

- ID registers.
- General system control registers.
- Debug registers.
- Generic Timer registers.
- Performance Monitors Registers.
- GIC CPU interface registers.


### 3.2.7 Memory model

The Cortex®-R82AE processor views memory as a linear collection of bytes numbered in ascending order from zero. For example, bytes 0-3 hold the first stored word, and bytes 4-7 hold the second stored word.

The Cortex®-R82AE processor can access halfwords, words, and doublewords in memory as either:


- Big-endian format.
- Little-endian format.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information about big-endian and little-endian memory systems.



**Note**

Some performance optimizations in the Cortex®-R82AE processor memory system are only activated when memory is accessed in little-endian format. For best performance, Arm recommends using the Cortex®-R82AE processor in little-endian format.



**Note**

Instructions are always little-endian.

#### 3.2.7.1 Memory types

The Arm®v8 architecture provides mutually exclusive memory types. System registers in *Memory Protection Unit* (MPU) define the memory types and attributes for each region in the memory map.

The memory types are:

<b>Normal</b>	This is generally used for bulk memory, both read/write and read-only.
<b>Device</b>	This is generally used for peripherals, which might be read-sensitive or write-sensitive. The Arm architecture restricts how accesses to Device memory may be ordered, merged, or speculated.

The Arm®v8 architecture divides Device memory into several subtypes. These relate to the following attributes:

<b>G</b>	Gathering. The capability to gather and merge requests together into a single transaction.
<b>R</b>	Reordering. The capability to reorder transactions.
<b>E</b>	Early Write Acknowledgement. The capability to accept early acknowledgement of transactions from the interconnect.

The following table describes the Arm®v8 architecture memory types.

**Table 3-3: Arm®v8 architecture memory types**

Memory type	Comment
GRE	Similar to Normal non-cacheable, but does not permit speculative accesses.
nGRE	Treated as nGnRE inside the Cortex®-R82AE processor, but can be reordered by the external interconnect.
nGnRE	Corresponds to Device in the Armv7 architecture.
nGnRE	Corresponds to Strongly Ordered in Arm® Armv7 architecture. Treated the same as nGnRE inside the Cortex®-R82AE processor, but reported differently on the bus sideband signals.

### 3.2.7.2 Memory system architecture

The Arm®v8-R AArch64 architecture supports the following memory system architectures:

- *Protected Memory System Architecture* (PMSA) at both EL1 and EL2. This is mandatory.
- *Virtual Memory System Architecture* (VMSA) at EL1. This is optional.

The Arm®v8-R AArch64 architecture allows either of the following memory system configurations for an implementation:

- PMSA at EL1 and PMSA at EL2.
- PMSA and VMSA at EL1 and PMSA at EL2.

The hypervisor running at EL2 can select the memory system architecture for each guest OS. This enables the hypervisor to support multiple guest operating systems utilizing either PMSA or VMSA on a per guest basis.

The Arm®v8-R AArch64 architecture supports two translation regimes:

- EL1 MPU or MMU handles stage 1 translation of EL1 and EL0 translation regime.
- EL2 MPU handles stage 1 translation of EL2 translation regime and stage 2 translation of EL1 and EL0 translation regime.

If an implementation only supports PMSA at EL1, the *Virtual Address* (VA), *Intermediate Physical Address* (IPA), and *Physical Address* (PA) are all the same and translation operation reduces to memory attribute and permission checks.

### 3.2.8 Security model

The Arm®v8-R AArch64 architecture does not support the EL3 Exception level and therefore there is no Secure Monitor to support switching between accesses to Secure and Non-secure physical memory address space. The Arm®v8-R AArch64 architecture always operates in Secure state at all Exception levels.

The Arm®v8-R AArch64 architecture supports two Secure translation regimes that determine whether the output address is in Secure or Non-secure physical memory address space. This

means that the Cortex®-R82AE processor always operates in Secure state but the Cortex®-R82AE processor can access both Secure and Non-secure physical memory address space.

### 3.3 Advanced SIMD and floating-point

Advanced SIMD is a media and signal processing architecture.

Floating-point performs half-precision, single-precision, and double-precision floating-point operations.



The Advanced SIMD architecture, its associated implementations, and supporting software, are also referred to as Arm® Neon™ technology.

---

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

## 4. Clocks and resets

This chapter describes the clocks and resets of the Cortex®-R82AE processor.

### 4.1 Clocks and clock enables

The Cortex®-R82AE processor requires clock signals for the cores, internal logic, and external interfaces. The Cortex®-R82AE processor provides clock enables on some interfaces allowing them to operate at an integer division of the main processor clock.

The Cortex®-R82AE processor is organized as a single cluster containing up to 8 cores that runs synchronously to the external memory system.

All clocks can be driven fully asynchronously to each other. The Cortex®-R82AE processor contains all the necessary synchronizing logic for crossing between clock domains. There are no clock dividers and no latches in the design. The entire design uses the rising edge of the clock.

The following table describes the Cortex®-R82AE processor clock input and output signals.

**Table 4-1: Clock signals**

Signal	Description
SCLK	The main system clock for all cluster and core logic including the memory system interfaces and the GIC interface.
PCLK	The clock for the DebugBlock and the debug APB interface in the cluster.  <b>Note:</b> The DebugBlock and the Cortex®-R82AE processor both have PCLK inputs. You might choose to connect these to the same clock. Alternatively, you might choose to place an asynchronous bridge between the two components, in which case they might be different clocks.
ATCLK	The clock for the ATB trace bus outputs from the cluster.
PERIPHCLK	The clock for Utility bus and peripheral logic inside the cluster such as timers, clock management logic, and power management logic.

In systems with DCLS and Split-Lock, the Cortex®-R82AE processor provides additional, redundant clocks for functional safety. They must be functionally identical to their primary counterpart. They must be driven with the same frequency and phase as their counterparts. There are no redundant debug and trace clocks because debug and trace are expected to be disabled during safe operation.

Redundant clock inputs must be provided for the Cortex®-R82AE processor configurations where `CIMODE > 0` regardless of the current `CFGCEMODE` signal configuration.

The following table describes the redundant clock input signals for functional safety.

**Table 4-2: Redundant clock signals**

Signal	Description
SCLKCHK	Functionally identical to SCLK.
PCLKCHK	Functionally identical to PCLK.
ATCLKCHK	Functionally identical to ATCLK.
PERIPHCLKCHK	Functionally identical to PERIPHCLK.

The Cortex®-R82AE processor provides clock enable inputs for the following interfaces to allow implementation of external logic to run at a lower synchronous frequency.

- *Main Manager* (MM) interface.
- *Main Accelerator Coherency Port* (MACP) subordinate interface.
- *Low-latency RAM* (LLRAM) manager interface.
- *ACE-Lite Subordinate* (ACELS) interface.
- *Shared Peripheral Port* (SPP) manager interface.
- *Low-latency Peripheral Port* <m> (LLPP<m>) manager interface.
- *Generic Interrupt Controller* (GIC) AXI5-Stream interface.
- Timers interface.

These interfaces can be timed as multicycle paths when they operate at an integer division of the main clock by using clock enable signals, including the paths through the interface to the *Dual-Core Lock-Step* (DCLS) delay logic. That is, the appropriate DCLS delay logic can only be enabled when the associated clock enable is asserted.

The following table describes the clock enable input signals and their scope.

**Table 4-3: Clock enable signals**

Signal	Scope
ACLKENM	MM interface
ACLKENA	MACP subordinate interface
ACLKENL	LLRAM manager interface
ACLKENS	ACELS interface
CLKEND	SPP manager interface
ACLKENP<m>	LLPP<m> manager interface
CLKENG	GIC AXI5-Stream interface
CNTCLKEN	Timers clock enable.

While there is no functional requirement for the clocks to have any relationship with each other, the Cortex®-R82AE processor is designed with the following assumptions to achieve optimal performance and minimize latency:

- SCLK should be set to the maximum achievable frequency for the optimal system performance.

- SCLK can run at synchronous n:1 frequency with the external interconnect, avoiding the need for an asynchronous bridge between them.
- SCLK can run at synchronous n:1 frequency with the external GIC, avoiding the need for an asynchronous bridge between them.
- PCLK and ATCLK can run at the same frequency as the relevant SoC components that they connect to. This would typically be approximately 25% of the maximum SCLK frequency.
- PERIPHCLK contains the architectural timers, and software performance can be impacted if reads to these registers take too long. Therefore, Arm® recommends that PERIPHCLK is run at least 25% of the maximum SCLK frequency.

### DCLS clock restrictions

When Lock-mode and Hybrid-mode execution modes are used, then the following additional clock restrictions apply:

- Due to DCLS timeout mechanisms, there is a constraint on the maximum clock ratio that is supported between any two clocks. This maximum supported clock frequency ratio is 20:1. For more details, see the table of the supported clock domain crossings below.
- The PERIPHCLK must have an equal or lower frequency than all other clocks.

R82AE contains the following clock domain crossings:

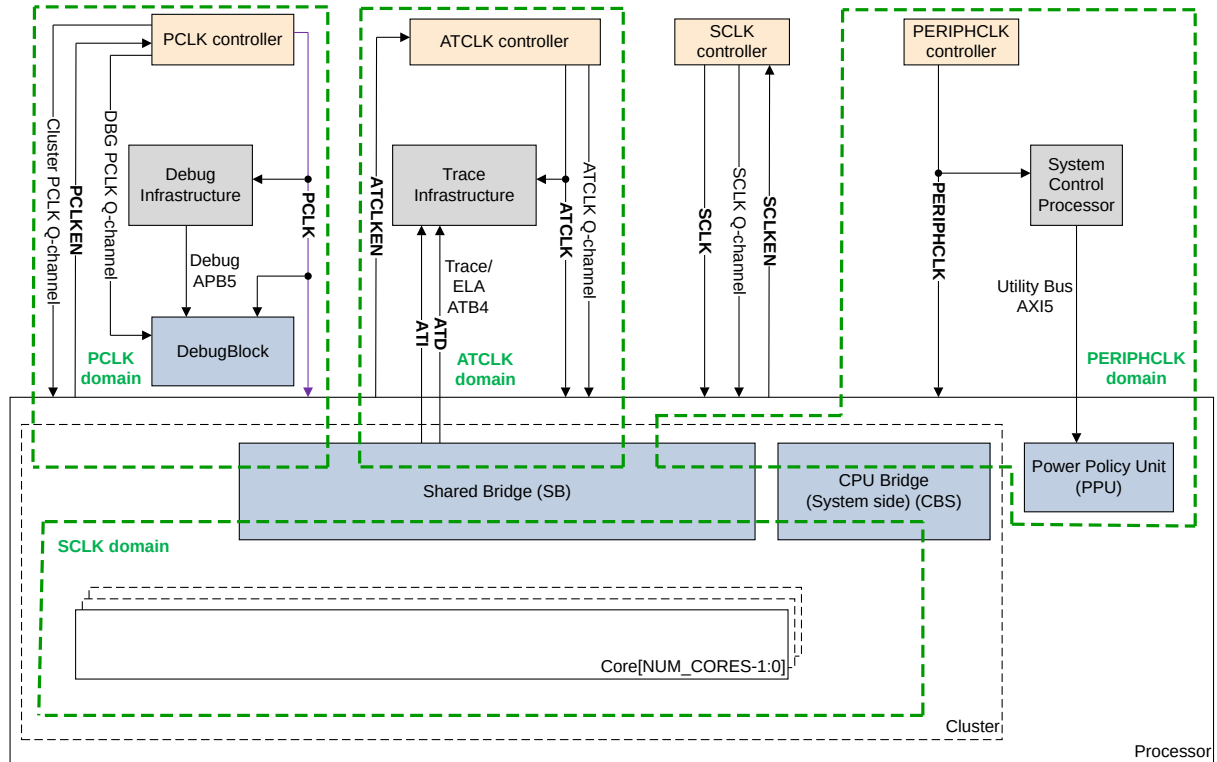
**Table 4-4: R82AE clock domain crossings**

Launching clock	Capturing clock
SCLK	PERIPHCLK
PCLK	PERIPHCLK
ATCLK	PERIPHCLK
PERIPHCLK	SCLK
PERIPHCLK	PCLK
PERIPHCLK	ATCLK

## 4.2 Clock domains

Most of the Cortex®-R82AE processor logic, including logic within each core, operates in a single clock domain, SCLK.

The following figure shows the Cortex®-R82AE processor clock domains and clock enable signals.

**Figure 4-1: Clock domains and clock enable signals****Note**

The DebugBlock is shown in a common PCLK domain with the cluster debug logic. However, the DebugBlock can be placed in a different clock domain provided asynchronous bridges are inserted on the APB interfaces between the DebugBlock and the cluster.

Each clock domain shown in the figure also outputs a clock enable signal. The clock enable signal is output from the *Power Policy Unit* (PPU) and indicates if the clock is required for that clock domain or not. For example, if the power domain associated with that clock domain is OFF, then the clock can be gated and Q-Channels ignored.

The following table describes the relationship between the clock enable signals, Q-Channel and the final clock.

xCLKEN	Q-state	Final clock
0	X (do not care)	0
1	Q_STOPPED	0
1	Q_RUN	1



## 4.3 Resets

The Cortex®-R82AE processor provides two cold (powerup) and active-LOW reset inputs and three warm (powered-on) and active-LOW reset outputs. The Cortex®-R82AE processor also provides programmable resets to allow resetting of individual parts of the design through integrated *Power Policy Units* (PPUs).

The following table describes the Cortex®-R82AE processor reset signals.

**Table 4-6: Reset signals**

Signal	Direction	Description
nRESET	Input	A global processor-wide Cold reset signal for all resettable registers in the SCLK domain excluding the DebugBlock.
nMBISTRESET	Input	A global processor-wide Cold reset signal for all resettable registers required for MBIST functionality (SCLK domain). It is intended for use by an external MBIST controller and allows it to avoid controlling the reset logic in the SoC.
nPRESET	Output	A reset signal for all resettable registers in the DebugBlock (PCLK domain).
nSRESET	Output	A reset signal for all resettable registers in the SCLK domain.
nATRESET	Output	A reset signal for all resettable registers in the ATCLK domain.

All reset inputs can be asserted (HIGH to LOW) and deasserted (LOW to HIGH) asynchronously for a minimum of 10 or more PERIPHCLK cycles. Reset synchronization logic inside the Cortex®-R82AE processor ensures that reset deassertion is synchronous for all resettable registers inside those reset domains. The clock does not need to be present for reset assertion and only PERIPHCLK (for the cluster) or PCLK (for the DebugBlock nPRESET) needs to be present for reset deassertion. However, the reset might not take effect in other clock domains until the relevant clock for that domain is active.



**Note**

You can use the Cortex®-R82AE processor reset output signals which are driven from the PPUs to reset any external logic that is in the same clock domain as the relevant parts of the cluster. For example, the nPRESET input to the DebugBlock can be connected to the nPRESET output of the cluster that is driven by the cluster PPU. This prevents possible synchronization problems. All the Cortex®-R82AE processor reset outputs are generated in the PERIPHCLK domain and therefore must be synchronized before use in the destination component.

When configured to support Lock or Hybrid modes (CIMODE set to 1,2 or 3), there are redundant reset inputs nRESETCHK and nMBISTRESETCHK. These are active-LOW and must be driven at the same time as the primary reset inputs.

The Cortex®-R82AE processor allows you to reset individual parts of the processor by programming the integrated PPUs. The following table describes the programmable resets. See [4.4 Resetting with PPUs](#) on page 70 on programming the PPU to control resets.

**Table 4-7: Programmable resets**

Programmable reset	Affected clock domains	Description
Core Cold reset	SCLK	Per-core Cold reset for all resettable registers in a specific core.
Core Warm reset	SCLK	Per-core Warm reset for all resettable registers in a specific core, except the Debug registers, ETM registers, and RAS registers.
Cluster Cold reset	SCLK, PCLK, ATCLK, PERIPHCLK	Cold reset for all resettable registers in the Cortex®-R82AE processor and the DebugBlock, except the PPU.
Cluster Warm reset	SCLK	Warm reset for all resettable registers in the Cortex®-R82AE processor, except the DebugBlock, the PPU, and the logic for the Utility bus, debug, ETM, and RAS functionality.

The Cortex®-R82AE processor has per-core CPUHALT<m> input pins. When a core comes out of reset and is ready to start fetching from the reset vector, it checks the value of its corresponding CPUHALT<m> input pin:

- While CPUHALT<m> is HIGH, the core waits and does not start fetching from the reset vector.
- While CPUHALT<m> is LOW, the core starts fetching from the reset vector and thereafter ignores CPUHALT<m>.

You can use the CPUHALT<m> pins to enable preloading of the *Instruction Tightly Coupled Memories* (ITCMs) via the ACLES interface while the CPU is under halt, such that the cores can boot from them.

The Cortex®-R82AE processor provides additional, redundant resets for functional safety, nRESETCHK and nMBISTRESETCHK. nRESETCHK is functionally identical to nRESET and nMBISTRESETCHK is functionally identical to nMBISTRESET. There are no redundant reset signals for debug and ETM because they are assumed to be disabled during safe operation.

## 4.4 Resetting with PPUs

The *Power Policy Units* (PPUs) control the power management features of the cluster and cores using a software interface. There is one PPU for the cluster and one for each core within the Cortex®-R82AE processor.

Certain power state changes, for example, powering up the cluster from a powered down state, includes implicit resets to internal logic. This internal reset is managed by the PPU controlling the transition between the two state modes and does not require an external signal to be asserted or explicit programming of the PPU. For more information on what internal reset actions result from power mode changes, see [6.7 Explicit resetting of cluster and cores and debug recovery](#) on page 105.

## 5. Power management

This chapter describes the power domains and the power modes in the Cortex®-R82AE processor.

### 5.1 About power management

The Cortex®-R82AE processor provides mechanisms to minimize both dynamic and static power dissipation.

The dynamic power management is achieved through local, regional, and architectural clock gating.

The static power management is achieved through dynamic retention capabilities enabled by multiple power domains and modes.

### 5.2 Voltage domain

The Cortex®-R82AE processor has one voltage domain.

The DebugBlock typically resides in the same voltage domain as the Cortex®-R82AE processor. However, you can place the DebugBlock in a separate voltage domain if necessary. In this case, the implementer has to place appropriate bridges on the APB interfaces between the DebugBlock and the Cortex®-R82AE processor.

### 5.3 Clock gating

The Cortex®-R82AE processor includes extensive clock gating to reduce dynamic power consumption.

Clock gating includes:

- Local clock gating inferred by the synthesis tools.
- Regional clock gating with instantiated clock gates covering a larger region of logic. As a subset of this, the Cortex®-R82AE processor implements architectural clock gating, defined as clock gating the majority of a core's logic when that core is in a low-power state, such as the *Wait for Interrupt* (WFI) state.
- Hierarchical clock gating which is performed externally to the Cortex®-R82AE processor when all components on a clock domain are idle.

### 5.3.1 Local and regional clock gating

The local and regional clock gating is performed automatically and needs no external support.

The Cortex®-R82AE processor has been designed to enable synthesis tools to automatically infer local clock gates for groups of flip-flops. These clock gates disable the clock and therefore reduce the dynamic power that is consumed by the flip-flops and logic local to the clock gate.

Regional clock gating in the Cortex®-R82AE processor allows the clock for larger regions of logic to be disabled when idle, which further reduces dynamic power consumption. The Cortex®-R82AE processor contains regional clock gates for all components within the cluster. The Cortex®-R82AE processor automatically enables and disables the regional clock gates according to its functional requirements.

The Cortex®-R82AE processor also implements architectural clock gating for the clock to a core when that core is in a low-power state, such as when executing a *Wait for Interrupt* (WFI) or *Wait for Event* (WFE) instruction. The architectural clock gates for each core are implemented within the CPU Bridge unit. The Cortex®-R82AE processor automatically enables and disables the architectural clock gates according to its functional requirements.

### 5.3.2 Hierarchical clock gating

The Cortex®-R82AE processor allows further power savings by supporting the clock to be gated off higher up in the clock tree. To do this, the Cortex®-R82AE processor provides Q-Channels for SCLK, ATCLK, and PCLK clock domains that can be used by an external clock controller to gate the clock when all components in that clock domain are idle.



There are two Q-Channels to hierarchically gate PCLK components, one for the cluster logic and one for the DebugBlock. This is because the DebugBlock can be implemented in a separate power domain and can be independently powered off and on.

---

The exception to this is the PERIPHCLK, because the PERIPHCLK is expected to drive the logic that is always ON and that is responsive to the events such as timers.

The Cortex®-R82AE processor has several interfaces that connect to other components in the SoC that are likely to be in the same clock domains. For example, the Cortex®-R82AE processor *Generic Interrupt Controller* (GIC) CPU interface signals might be in the same clock domain as the external GIC distributor, and the Cortex®-R82AE processor ATB interface signals might be in the same clock domain as the external trace infrastructure. Hierarchical clock gating of these components when they are idle allows further power reduction.

Most of the Cortex®-R82AE processor, including the logic within each core, operates in a single clock domain, SCLK. When all cores and all cluster components are inactive, a Q-Channel allows an external clock controller to gate the whole SCLK domain.

The hierarchical clock gates are implemented within the *Shared Bridge* (SB) unit.

### 5.3.2.1 Wait for Interrupt and Wait for Event

*Wait for Interrupt* (WFI) and *Wait for Event* (WFE) are architectural features that are used to put each core in the Cortex®-R82AE processor in a low-power Standby mode by regional disabling the clock at the top of the clock tree.

To reduce dynamic power, each core in the Cortex®-R82AE processor can request entry into a low-power state using the `WFI` and `WFE` instructions. In the low-power state, most of the clocks in a core are disabled while keeping the core powered up. This reduces the power drawn to the static leakage current, leaving a small clock power overhead to enable the core to wake up.

In addition to the per-core `WFI` and `WFE` low-power states, the clock to (almost all) the L2 and *LLRAM Coherency Unit* (LCU) logic is automatically disabled when the cluster is sufficiently idle.

A `WFI` or `WFE` instruction completes when:

- All outstanding load instructions are completed.
- All store instructions are completed.
- All cache and *Translation Lookaside Buffer* (TLB) maintenance operations are completed.
- All bus traffic is completed.

While a core is in the low-power state, the clocks in the core are temporarily enabled under the following conditions:

- A snoop request from the L2 cache that must be serviced by the L1 data cache.
- A cache or TLB maintenance operation that must be serviced by the core L1 caches.
- An APB access to the debug, trace, or core *Performance Monitoring Unit* (PMU) registers residing in the core power domain.
- An access request from the *Generic Interrupt Controller* (GIC) distributor to the GIC CPU interface.
- An access from the Utility bus to *Reliability, Availability, and Serviceability* (RAS) registers.

While the clocks in the core are temporarily enabled, the core remains in the `WFI` or `WFE` low-power state.

#### WFE wake up event signaling

- A *Send Event* (`SEV`) instruction signals a `WFE` wake up event to other clusters by asserting the `EVENTOREQ` output.
- The `EVENTIREQ` input indicates that another cluster or system component has signaled a `WFE` wake up event.

## System global exclusive monitor signaling

Any global exclusive monitor in the system must be able to generate an event when it is cleared. This event must be signaled to the cluster using the EVENTIREQ input.

## 5.4 Power domains

The Cortex®-R82AE processor supports several different power domains. However, you do not need to implement all the available power domains. The implementation choices, such as the number of cores or L2 cache implementation, determine the number and type of power domains that are able to be implemented.

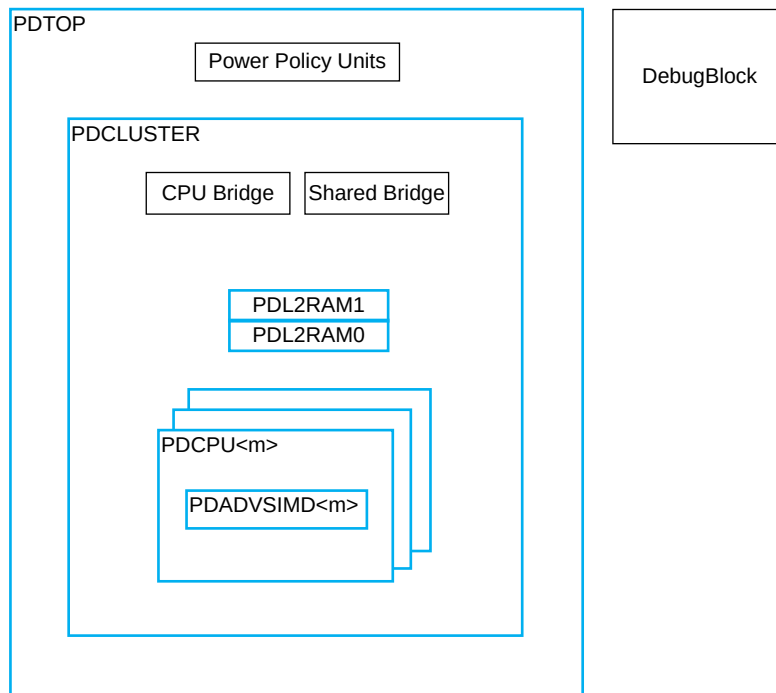
The Cortex®-R82AE processor supports PDTOP, PDCLUSTER, PDL2RAM0, PDL2RAM1, PDCPU<m>, and PDADVSIMD<m> power domains.



PDADVSIMD<m> is present if the core <m> is configured to support Advanced SIMD and floating-point (`NEON_FP<m> = 1`).

---

The following figure shows the supported power domains. Each box with blue boundaries indicates a separate power domain.

**Figure 5-1: Processor power domains**

## PDTOP

The Cortex®-R82AE processor has a top-level power domain, PDTOP, that allows the whole processor to be turned off. PDTOP is expected to be in the same power domain as other SoC components. The only cluster logic in PDTOP power domain is the *Power Policy Units* (PPUs) which will typically be always On. This is because the PPUs need to power down the other power domains including PDCLUSTER while remaining active.

The PDTOP power domain must be powered up before any of the other power domains are powered up. It must only be powered down after the other power domains have been powered down.

The DebugBlock is designed to be included in a separate Debug power domain with other Debug components.

## PDCLUSTER

The whole cluster, excluding the PPUs, belongs to a single power domain, PDCLUSTER. This allows the Cortex®-R82AE processor to be put in a lower power state while the PPUs stay operational to handle power transitions.

## PDL2RAM0 and PDL2RAM1

PDL2RAM0 and PDL2RAM1 power domains enable the independent power control of the L2 cache RAMs. PDL2RAM0 and PDL2RAM1 power domains allow:

- The L2 cache to support operation with only half of the RAMs active, when multiple cores are turned off or in retention.



PDL2RAM0 and PDL2RAM1 can be controlled individually only if `L2_SLICES` is set to 2.

- The Cortex®-R82AE processor to turn off or put in retention all the L2 cache RAMs.

### PDPCPU<m>

Each core within the Cortex®-R82AE processor has its own power domain, PDPCPU<m>, to allow the cores to be powered down individually.

### PDADVSIMD<m>

The Advanced SIMD and floating-point block in each core within the Cortex®-R82AE processor is also part of the power domain for that core. However, to support independent retention control, each Advanced SIMD and floating-point block also has its own power domain, PDADVSIMD<m>, for isolating it from the surrounding domain. This allows the Advanced SIMD and floating-point block to be put in retention while the rest of the core is active.

Clamping and isolation cells between power domains are inferred from the supplied UPF files rather than instantiated in the RTL.

The following table shows the power domains that the Cortex®-R82AE processor supports.

**Table 5-1: Power domain description**

Power domain	Description
PDTOP	This domain contains all cluster logic including the <i>Power Policy Units</i> (PPUs).
PDCLUSTER	This domain contains the <i>Shared Bridge</i> (SB), <i>CPU Bridge</i> (CB) (both system side and CPU side CBs), trace and debug routing infrastructure, <i>LLRAM Coherency Unit</i> (LCU), <i>Shared AXI Subordinate Unit</i> (SAXIS), L2 coherency logic, and L2 cache RAMs. It excludes the PPUs.
PDL2RAM0	This domain contains the first half of the L2 cache RAMs.
PDL2RAM1	This domain contains the second half of the L2 cache RAMs.
PDPCPU<m>	This domain contains all core logic including the optional Advanced SIMD and floating-point block, the <i>Tightly Coupled Memories</i> (TCMs) and L1 cache RAMs, and Debug registers that are associated with the core <m> where m is the core number in the range of 0-7.  If a core is not present, the corresponding power domain is not present.
PDADVSIMD<m>	This is a power domain for Advanced SIMD and floating-point block in core <m> to implement functional retention.  <m> is the core number in the range of 0-7. If the Advanced SIMD and floating-point block is not present in core <m>, the PDADVSIMD<m> power domain is not present.



## 5.5 Power mode control

Power mode control is distributed between power management software, the cluster, and the *Power Policy Units* (PPUs) integrated within the cluster.

A component in the SoC such as a *System Control Processor* (SCP) can program the PPU over the Utility bus to set the appropriate power policy. If your system does not have an SCP component, the Utility Bus can be connected to one of the Cortex®-R82AE processor ports or to your SoC interconnect, so one of the cores in the Cortex®-R82AE processor can program the PPUs.

If your system does not need to perform any power transitions, the Cortex®-R82AE processor can also be configured so that the PPUs are powered on at reset and never require any programming. See [6.9 Implications of not having a System Control Processor](#) on page 110 for more information on Cold reset state for the PPUs.

The PPUs control the low-level details of powering up, powering down, or resetting domains as necessary to implement the requested policy. The hardware performs any actions necessary to reach the requested power mode, such as gating clocks, flushing caches, or disabling coherency.

The power mode of each core can be changed independently of other cores in the cluster, however the cluster power mode is linked to the state of the cores. There is no requirement on the order that cores are powered on or off.

The PPUs and cluster logic perform all the logical functions needed to enter or exit a power mode. However, there are some steps related to the physical state such as controlling power switches or retention states. The logic to carry out these steps is not included in the Cortex®-R82AE processor, because it varies depending on the technology process, library, and internal design rules. Therefore the implementer must provide a *Power Control State Machine* (PCSM) that sequences these implementation-specific steps.

The PPU interfaces to the PCSM via a P-Channel interface, where the PPU can initiate a request to a new power mode. The PCSM accepts that request when it has completed all of its required actions.

Software sets the operating requirements by writing to the following System registers:

### **Cluster Power Control Register (IMP\_CLUSTERPWRCTLR\_EL1)**

To request partial L2 cache powerup or powerdown and to enable RAM retention capabilities.

### **Cluster Powerdown Register (IMP\_CLUSTERPWRDN\_EL1)**

To request the power mode that the cluster is to enter after all cores have powered off. For example, memory retention mode.

### **CPU Power Control Register (IMP\_CPUPWRCTLR\_EL1)**

To request core powerdown and to enable Advanced SIMD and floating-point retention capabilities.

## 5.6 Debug over powerdown

The Cortex®-R82AE processor supports debug over powerdown which allows a debugger to retain its connection with the Cortex®-R82AE processor even when the Cortex®-R82AE processor is powered down. This behavior enables debug to continue through powerdown scenarios rather than having to re-establish a connection each time the Cortex®-R82AE processor is powered up.

The debug over powerdown logic is part of the DebugBlock which is external to the Cortex®-R82AE processor. The DebugBlock is provided as a separate component to allow implementation in a separate power domain from the processor. Having a separate debug power domain allows the connection to a debugger be maintained while the cores and cluster are powered down.

## 5.7 Core power modes and transitions

Each core within the Cortex®-R82AE processor has a defined set of power modes and permitted transitions between these modes. The power mode of each core can be independent of other cores in the Cortex®-R82AE processor.

The following table shows the supported core power modes.



Note

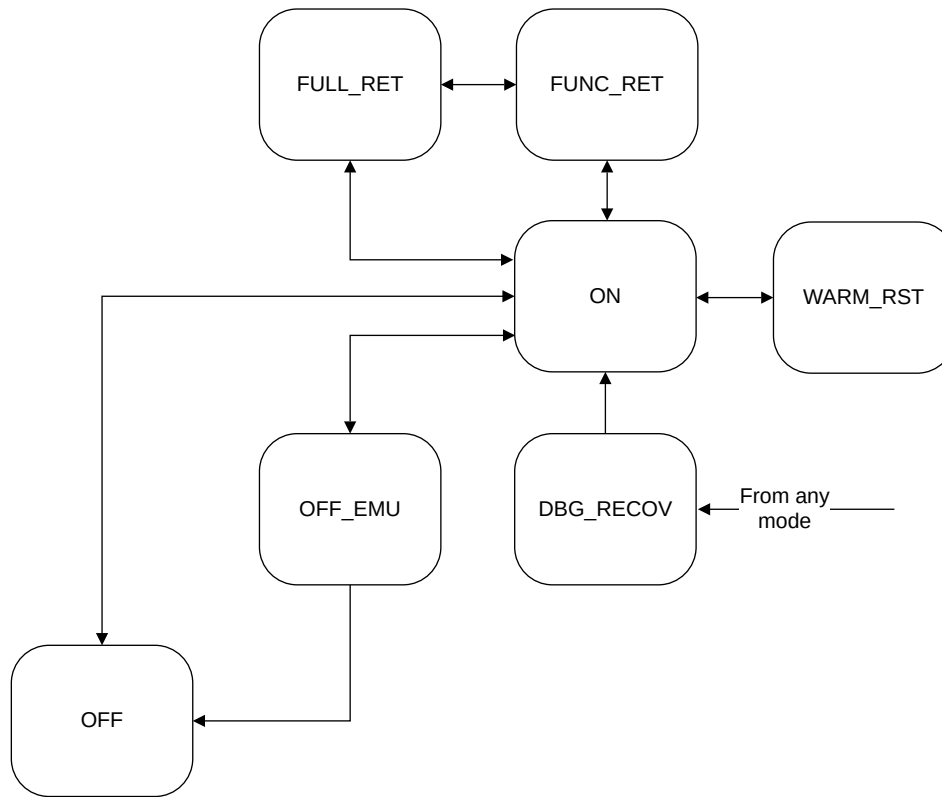
As part of the powerdown sequence any core in lock-step in the Cortex®-R82AE processor must disable and clear any interrupt outputs from the core, such as the timer interrupts. Failing to clear these interrupt outputs can lead to a false positive error report from the lock-step comparators.

**Table 5-2: Core power modes**

Power mode	Short name	Description
On	ON	The core is powered up and active.
Functional retention	FUNC_RET	The core is fully powered and operational, but the Advanced SIMD and floating-point logic is in retention.  All instructions except for Advanced SIMD and floating-point ones can execute normally. When an Advanced SIMD or floating-point instruction is encountered, the pipeline stalls until the core can transition to ON to execute the instruction.
Full retention	FULL_RET	The core and all the RAMs are in retention.  In this mode, only power that is required to retain register and RAM state is available.  The core must be in <i>Wait for Interrupt</i> (WFI) or <i>Wait for Event</i> (WFE) low-power state before it enters this mode.
Off	OFF	The core is powered down.

Power mode	Short name	Description
Emulated off	OFF_EMU	<p>Emulated off mode permits you to debug the powerup and powerdown cycle without changing the software.</p> <p>In this mode, the core powerdown is normal, except:</p> <ul style="list-style-type: none"> <li>• The clock is not gated and power is not removed when the core is powered down.</li> <li>• Only the Warm reset is asserted. The debug logic is preserved in the core and remains accessible by the debugger.</li> </ul> <p><b>Note:</b> Emulated off mode operation for the shared logic is identical to the operation for a core.</p>
Debug recovery reset	DBG_RECOV	<p>Debug recovery reset is used for applying a reset to the core, while preserving memory and optionally <i>Reliability, Availability, and Serviceability</i> (RAS), Debug, and Trace registers for debug purposes. The L1 cache state is preserved when transitioning from DBG_RECOV mode to ON mode. Debug recovery mode is typically used in debugging a watchdog timeout.</p> <p><b>Caution:</b> This mode must not be used during normal system operation.</p>
Warm reset	WARM_RST	<p>Warm reset is a best effort to recover from system level issues while keeping the state for the trace logic and the Debug and RAS registers.</p> <p><b>Caution:</b> This mode must not be used during normal system operation.</p>

The following diagram shows the supported power modes for each core and the permitted transitions between them.

**Figure 5-2: Core power mode transitions**

## ON

In this mode, the core is on and fully operational.

The core can be initialized into the On mode. When a transition to the ON mode completes, all caches are accessible and coherent. Other than the normal architectural steps to enable caches, no additional software configuration is required.

## FUNC\_RET

In this mode, the Advanced SIMD and floating-point logic is in retention (inoperable but with state retained) and the remainder of the core logic is operational.

This means that if an Advanced SIMD and floating-point instruction is executed while in this mode, it is stalled until the core enters the ON mode.

When the Advanced SIMD and floating-point logic is in retention, the clock to the logic is automatically gated outside of the retained domain.

You can control the FUNC\_RET by setting the IMP\_CPUPWRCTLR\_EL1.FPURET register bits.

## FULL\_RET

In this mode, all core logic and RAMs are in retention, that is the domain is inoperable but with core state retained.

This mode is typically used when the core is in *Wait for Interrupt* (WFI) or *Wait for Event* (WFE) state for an extended period of time.

When the core is in FULL\_RET, there is support for Snoop and debug access so the core transitions to the ON state to process the access. The core, then, transitions back to FULL\_RET without the core leaving WFI or WFE state.

The core dynamic retention can be enabled and disabled separately for WFI and WFE by software running on the core. You can program separate timeout values for entry into this mode from WFI and WFE mode:

- Use the IMP\_CPUPWRCTLR\_EL1.WFIRET register bits to program timeout values for entry into core FULL\_RET mode from WFI mode.
- Use the IMP\_CPUPWRCTLR\_EL1.WFERET register bits to program timeout values for entry into core FULL\_RET mode from WFE mode.

When the Cortex®-R82AE processor transitions a core from FULL\_RET to ON powermode:

- The L1 cache, L2 duplicate L1 tag RAM, and LCU duplicate L1 tag RAM are not invalidated.

## OFF

In this mode, all core logic and RAMs are unused and can be powered down. The domain is inoperable and all core state is lost.

When the core is in OFF, any attempted debug access returns an error response on the internal debug interface indicating the core is not available.

The core can enter the OFF mode by setting the IMP\_CPUPWRCTLR\_EL1.PWRDN register bit.

## OFF\_EMU

In this mode, all core logic and RAMs are kept physically powered on. However, core Warm reset is asserted externally to emulate OFF scenario while keeping core debug state and allowing debug access.

All Debug registers retain their state and are accessible from the external debug interface. All other functional interfaces behave as if the core were OFF.

## DBG\_RECOV

Debug recovery mode can be used to assist debug of external watchdog-triggered reset events.

In DBG\_RECOV mode, the core logic including the L1 cache RAMs is powered up.

All powered-on cores and the cluster need to be put into DBG\_RECOV mode. When this happens, the processor applies either a Warm reset or a Cold reset, depending on the PPU\_PTCR.DBG\_RECOV\_PORST\_EN value. Following this, the powered-on cores and cluster

should be put into the ON power mode. See [6.7 Explicit resetting of cluster and cores and debug recovery](#) on page 105 for more information.

Normally, the Cortex®-R82AE processor performs the following when there is a transition to ON power mode:

- Invalidates the L1 cache, L2 duplicate L1 tag RAM, and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAM (when there is a core transition from OFF, OFF\_EMU, or WARM\_RST to ON mode and a Warm reset or a Cold reset applies).
- Resets the register file and System registers which have an **UNKNOWN** reset value (when there is a core transition from OFF, OFF\_EMU, or WARM\_RST to ON mode and a Warm reset or a Cold reset applies).
- Resets the Debug, Trace and *Reliability, Availability, and Serviceability* (RAS) state (when there is a transition from OFF to ON mode and a Cold reset applies).

In contrast, when the Cortex®-R82AE processor transitions a core from DBG\_RECOV to ON power mode:

- The L1 cache, L2 duplicate L1 tag RAM, and LCU duplicate L1 tag RAM are not invalidated.
- The register file is not reset, unless flop parity is configured where the register file is always reset.
- System registers which have a defined reset value are reset, but System registers which have an **UNKNOWN** reset value are preserved, unless flop parity is configured where all System registers are reset regardless.
- If PPU\_PTCR.DBG\_RECOV\_PORST\_EN = 1, the Debug, Trace and RAS state is reset. If PPU\_PTCR.DBG\_RECOV\_PORST\_EN = 0, the Debug, Trace and RAS state is preserved.

Debug recovery mode can be entered from any other mode. The core *Power Policy Unit* (PPU) controls entry into this mode.



**Caution**

- The system must be able to program the PPUs over the Utility bus to use Debug recovery. For example, the system may have a *System Control Processor* (SCP), or the debug subsystem may connect to the Utility bus.
- Debug recovery mode is strictly for debug purposes. It must not be used for functional purposes, because correct operation of the caches is not guaranteed when entering this mode. To go back to functional mode, the system has to go through a full Cold reset.
- When executing in Lock-mode, some Warm resets might break lock-step execution and cause false DCLS faults to be reported after reset de-assertion.
- Debug recovery mode can occur at any time with no guarantee of the state of the core. A P-Channel request of this type is accepted immediately, therefore its effects on the core, cluster, or the wider system are **UNPREDICTABLE**, and a wider system reset might be required. In particular, if there were outstanding memory system transactions or shared System registers being accessed at the time of the reset, then these transactions might complete after the reset when the core is not expecting them and cause a system deadlock.

- No debug access to the core should be made in this power mode. Debug access should only be made in the ON or OFF\_EMU power mode.
- If the system sends a snoop to the cluster during debug recovery mode, then depending on the cluster state, the snoop might get a response and disturb the contents of the caches, or it might not get a response and cause a system deadlock.

---

## WARM\_RST

A Warm reset resets all state except for the trace logic and the debug and RAS registers.

A Warm reset invalidates the caches and snoop filters and resets the register file and System registers with **UNKNOWN** reset values.



- If any core is put into Warm reset mode, then the cluster must also be put into Warm reset mode and the other cores must go into Warm reset mode, Off mode, or Emulated off mode. Therefore, using the core Warm reset mode has the end result of resetting the cores and the shared logic.
  - When executing in Lock-mode, some Warm resets might break lock-step execution and cause false DCLS faults to be reported after reset de-assertion.
  - The system must be able to program the PPUs over the Utility bus to use Warm reset. For example, the system may use an SCP.
  - Warm reset is a best effort to recover from system level issues while keeping debug and RAS registers and should not be used for functional purposes.
  - No debug access to the core should be made in this power mode. Debug access should only be made in the ON or OFF\_EMU power mode.
  - Warm reset state can occur at any time for an ON core with no further guarantees of its state. A request of this type is accepted immediately by an ON core, therefore its effects on the core, cluster, or the wider system are **UNPREDICTABLE**, and a wider system reset might be required. In particular, if there were outstanding memory system transactions or shared System registers being accessed at the time of the reset, then these transactions might complete after the reset when the core is not expecting them and cause a system deadlock.
- 

## 5.8 Core powerdown

You must follow a specific powerdown sequence to trigger core powerdown.

To trigger core powerdown:

1. Save all architectural state.
2. Configure the *Generic Interrupt Controller* (GIC) distributor to disable or reroute interrupts away from the core.



GIC distributor can be either of the following:

- An Arm GIC distributor, such as GIC-625, that connects to the GIC Stream processor ports.
- Any other interrupt controller that might be driving the nFIQ, nIRQ, nVFIQ, or nVIRQ processor inputs.

3. Set the IMP\_CPUPWRCTLR\_EL1.PWRDN bit to 1 to indicate to the power controller that a powerdown is requested.
4. Execute an *Instruction Synchronization Barrier* (ISB) instruction.
5. Execute a `WFI` instruction.

After executing `WFI` and then receiving a powerdown request from the power controller, the hardware:

- Disables and flushes the L1 caches.
- Removes the core from coherency.

When the IMP\_CPUPWRCTLR\_EL1.PWRDN bit is set, executing a `WFI` instruction automatically masks all interrupts and wakeup events in the core. As a result, applying reset is the only way to wake up the core from the `WFI`.

No software steps are required to bring a core into coherence after reset.

## 5.9 Cluster power modes

The Cortex®-R82AE processor supports various cluster level low-power modes and includes hardware to handle power mode transitions with minimal software support.

The following table shows the supported power modes for the shared logic in the Cortex®-R82AE processor.

**Table 5-3: Cortex®-R82AE processor shared logic power modes**

Power mode	Short name	Description
On	ON	On mode is the normal mode of operation where all shared logic functionality is available.
Memory retention	MEM_RET	In Memory retention mode, only the L2 cache RAMs are placed in retention. The rest of the cluster including the L2 logic and the cores are powered down.
Emulated memory retention	MEM_RET_EMU	In Emulated memory retention mode, the cluster behaves logically as if it were in the MEM_RET mode, except that the shared RAMs and the cluster logic remain powered. The debug state is retained and is accessible.
Off	OFF	In Off mode, power is removed from the cluster logic and all the RAMs. Only the <i>Power Policy Units</i> (PPUs) remain powered.
Emulated off	OFF_EMU	In Emulated off mode, the cluster behaves logically as if it were in the OFF mode, except that the logic remains powered. The debug state is retained and accessible.



Power mode	Short name	Description
Debug recovery reset	DBG_RECOV	<p>Debug recovery reset is used for applying a reset to the cluster, while preserving memory and optionally <i>Reliability, Availability, and Serviceability</i> (RAS), Debug, and Trace registers for debug purposes. The L2 cache state is preserved when transitioning from DBG_RECOV mode to ON mode. Debug recovery mode is typically used in debugging a watchdog timeout.</p> <p><b>Caution:</b> This mode must not be used during normal system operation.</p>
Warm reset	WARM_RST	<p>The Warm reset mode provides a Warm reset to all the shared cluster logic apart from the <i>Power Policy Units</i> (PPUs).</p> <p>Warm reset is a best effort to recover from system level issues while keeping the state for the trace logic and the Debug and RAS registers.</p> <p><b>Caution:</b> This mode must not be used during normal system operation.</p>

## ON

In this mode, the cluster is on and fully operational.

When a transition to the ON mode completes, the L2 cache is accessible and coherent without needing any configuration from software other than the normal architectural steps to enable caches.

## MEM\_RET

In Memory retention mode, the L2 cache RAMs are placed in retention while the shared logic and the cores are powered down.

It is quicker for the cluster to enter and exit MEM\_RET mode as compared with going from OFF to ON mode or ON to OFF mode, for example in powerup or powerdown. This is because, the L2 cache RAMs do not need to be cleaned and the data later reloaded. Placing the L2 cache RAMs in retention also saves on energy required to write dirty data back to main memory.



**Caution**

The Cortex®-R82AE processor remains in coherence when in MEM\_RET mode. Therefore, when using this mode, beware that if other external coherent agents are active, it takes considerable time for them to access to the L2 cache RAMs. Although it is possible for external agents in the system to access the L2 cache RAMs while in retention, it comes at considerable time cost because the Cortex®-R82AE processor needs to be temporarily powered up to service the access.

When the Cortex®-R82AE processor transitions the cluster from MEM\_RET to ONmode:

- The L2 cache, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs are not invalidated.

## MEM\_RET\_EMU

In Emulated memory retention mode, the cluster behaves logically as if it were in the MEM\_RET mode except that the cluster shared logic remains powered. This means the L2 cache RAMs, L2 duplicate L1 tag RAMs, *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs, and the rest of the cluster logic remains powered. Therefore, debug accesses can be made.

## OFF

In the OFF mode, all the shared cluster logic including the L2 duplicate L1 tag RAMs, LCU duplicate L1 tag RAMs, L2 cache RAMs, and the cores are powered down. The PDCLUSTER domain is inoperable and all state is lost.

In the OFF mode, power is removed from PDCLUSTER power domain but the PDTOP power domain is still powered up including all the *Power Policy Units* (PPUs).

The Cortex®-R82AE processor can be initialized into this mode on a Cold reset.

## OFF\_EMU

In this mode, the cluster behaves logically as if it were in the OFF mode. However, the cluster shared logic remains powered including the L2 cache RAMs, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs. Therefore, debug accesses to the cluster can still be made.

In this mode, the cluster behaves as if it were powered off for functional logic, but it allows the cluster to maintain debug access. On entering this mode, a Warm reset is applied to the cluster, resetting the functional logic but not resetting the debug logic. From the perspective of software running on the core, the cluster appears to be powered off.

## DBG\_RECOV

The Debug recovery mode can be used to assist debug of external watchdog-triggered reset events.

In DBG\_RECOV mode, all the Cortex®-R82AE processor shared logic including the L2 cache RAMs is powered up.

All powered-on cores and the cluster need to be put into DBG\_RECOV mode. When this happens, the processor applies either a Warm reset or a Cold reset, depending on the CLUSTERPPU\_PTCR.DBG\_RECOV\_PORST\_EN value. Following this, the powered-on cores and cluster should be put into the ON power mode. See [6.7 Explicit resetting of cluster and cores and debug recovery](#) on page 105 for more information.

Normally, the Cortex®-R82AE processor performs the following when there is a transition to ON power mode:

- Invalidates the L2 cache, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs (when there is a cluster power mode transition from OFF, OFF\_EMU, or WARM\_RST to ON mode and a Warm reset or a Cold reset applies)
- Resets the Debug, Trace and *Reliability, Availability, and Serviceability* (RAS) state (when there is a cluster power mode transition from OFF to ON mode and a Cold reset applies).

In contrast, when the Cortex®-R82AE processor transitions the cluster from DBG\_RECOV to ON mode:

- The L2 cache, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs are not invalidated.
- System registers which have a defined reset value are reset, but System registers which have an **UNKNOWN** reset value are preserved, unless flop parity is configured where all System registers are reset regardless.
- If CLUSTERPPU\_PTCR.DBG\_RECOV\_PORST\_EN = 1, the Debug, Trace and RAS state is reset. If CLUSTERPPU\_PTCR.DBG\_RECOV\_PORST\_EN = 0, the Debug, Trace and RAS state is preserved.

Debug recovery mode can be entered from any other mode. The cluster *Power Policy Unit* (PPU) controls entry into this mode.



Caution

- The system must be able to program the PPUs over the Utility bus to use Debug recovery. For example, the system may have a System Control Processor (SCP), or the debug subsystem may connect to the Utility bus.
- Debug recovery mode is strictly for debug purposes. It must not be used for functional purposes because correct operation of the cluster is not guaranteed when entering this mode. To go back to functional mode, the system has to go through a full Cold reset.
- When executing in Lock-mode, some Warm resets might break lock-step execution and cause false DCLS faults to be reported after reset de-assertion.
- No debug access to the cluster should be made in this power mode. Debug access should only be made in the ON or OFF\_EMU power mode.
- Debug recovery mode can occur at any time with no guarantee of the state of the cluster. A request of this type is accepted immediately, therefore its effects on the core, cluster, or the wider system are unpredictable and a wider system reset might be required. In particular, if there were outstanding memory system transactions or shared System registers being accessed at the time of the reset, then these transactions might complete after the reset when the cluster is not expecting them and cause a system deadlock.

If the system sends a snoop to the cluster during this mode, then depending on the cluster state:

- The snoop might get a response and disturb the contents of the caches.
- The snoop might not get a response and cause a system deadlock.
- In the following cases, it might not be possible to enter DBG\_RECOV without a Cold reset of the cluster:
  - When the cluster is in middle of a power transition which cannot complete because of the system hanging or trying to debug.
  - When the cluster is in the middle of a clock gating transition on the SCLK Q-Channel which cannot complete because of the system hanging or trying to debug.
  - The cluster is in Warm reset.

- You must choose the correct operating mode corresponding to the L2 cache partitions and L2 cache slices that were in use before Debug recovery mode.

---

## WARM\_RST

A Warm reset resets all state except for the trace logic and the debug and RAS registers.

A Warm reset invalidates the caches and snoop filters and resets the register file and System registers with **UNKNOWN** reset values.



- If any core is put into Warm reset mode, then the cluster must also put into Warm reset mode and the other cores must go into Warm reset mode, Off mode, or Emulated off mode. Therefore, using cluster Warm reset mode has the end result of resetting the cores and the shared logic.
- When executing in Lock-mode, some Warm resets might break lock-step execution and cause false DCLS faults to be reported after reset de-assertion.
- The system must be able to program the PPU over the Utility bus to use Warm reset. For example, the system may use an SCP.
- Warm reset is a best effort to recover from system level issues while keeping debug and RAS registers and should not be used for functional purposes.
- No debug access to the cluster should be made in this power mode. Debug access should only be made in the ON or OFF\_EMU power mode.
- Warm reset mode is only expected to be used for resets triggered by a system level issue, such as a watchdog timeout, and therefore a Cold system reset might be required. In particular, if there were outstanding memory system transactions or shared System registers being accessed at the time of the reset, then these transactions might complete after the reset when the cluster is not expecting them and cause a system deadlock.
- The warm reset power mode can occur at any time with no further guarantees for the state of the cluster. A request of this type is accepted immediately by the cluster, therefore its effects on the core, cluster, or the wider system are **UNPREDICTABLE**, and a wider system reset might be required. In particular, if there were outstanding memory system transactions or shared System registers being accessed at the time of the reset, then these transactions might complete after the reset when the core is not expecting them and cause a system deadlock.

---

## 5.10 Cluster operating modes

An operating mode is a component-specific configuration of the power modes. For the Cortex®-R82AE processor, the operating modes differ in the amount of L2 cache RAM that is active.

The cluster *Power Policy Unit* (PPU) provides programming access to control the operating modes and the power modes.

The Cortex®-R82AE processor supports three operating modes.

The following table shows the operating modes for the L2 cache RAMs.

**Table 5-4: Operating modes for L2 cache RAMs**

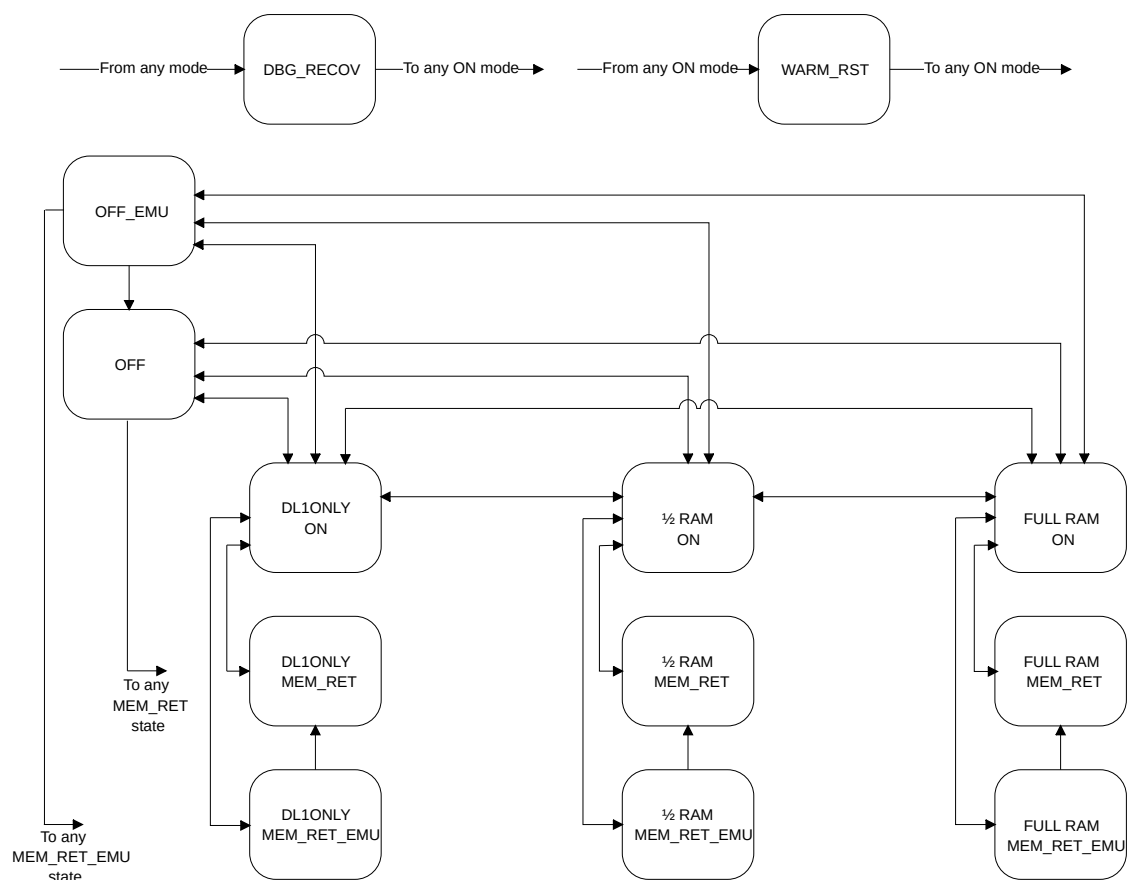
Operating mode	Short name	Description
L2 duplicate L1 tag RAM and <i>LLRAM Coherency Unit</i> (LCU) duplicate L1 tag RAM only	DL1ONLY	The L2 cache partition in each cache slice is powered down
Half L2 cache	½ RAM	One half of the L2 cache partition in each active slice is powered up <b>Note:</b> This mode is possible only if <code>L2_SLICES</code> is set to 2.
Full L2 cache	FULL RAM	All of the L2 cache partition in each active slice is powered up

## 5.11 Cluster PPU mode transitions

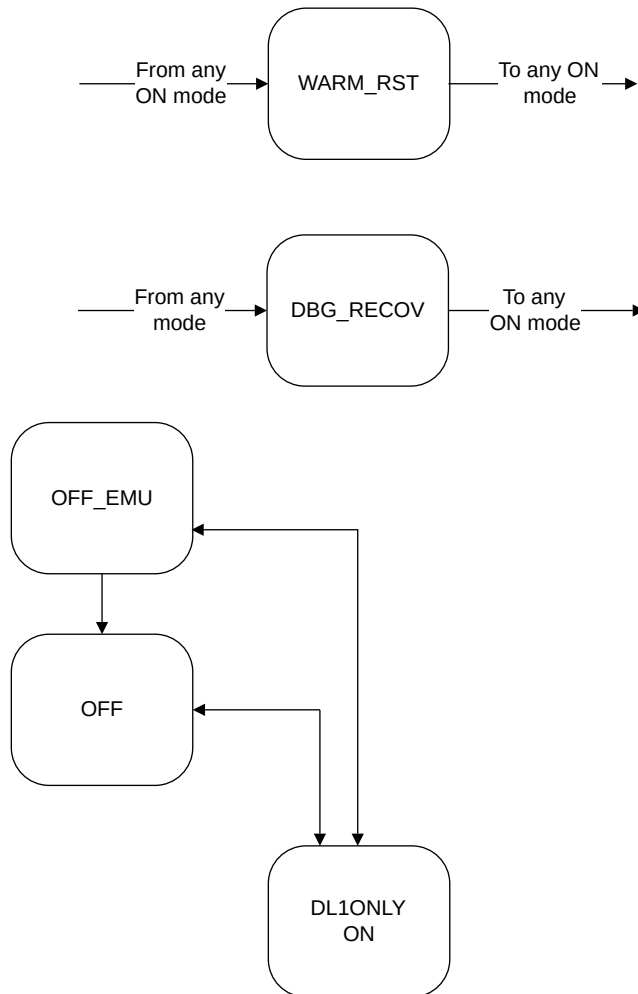
The Cortex®-R82AE processor supports transitions between cluster power modes and cluster operating modes. Each combination of cluster power mode with an L2 cache RAM operating mode forms a *Power Policy Unit* (PPU) mode, for example, FULL RAM ON. Individual power modes such as ON, OFF, and OFF\_EMU are also considered to be PPU modes.

The cluster PPU controls transitions between the PPU modes. Therefore, a *System Control Processor* (SCP) or any core within the Cortex®-R82AE processor through a Utility bus loopback connection can program up the PPU to go to any PPU mode and the PPU would automatically schedule the necessary transitions to achieve that PPU mode.

The following figure shows the supported PPU mode transitions for the Cortex®-R82AE processor.

**Figure 5-3: Cortex®-R82AE cluster PPU mode transitions**

The following figure shows the supported PPU mode transitions for the Cortex®-R82AE processor where the L2 cache is not implemented.

**Figure 5-4: Cortex®-R82AE cluster PPU mode transitions, no L2****FULL RAM ON**

In this PPU mode, all the shared logic including the L2 cache RAMs, L2 duplicate L1 tag RAMs, *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs, and PPUs is powered up and fully operational. When a transition to the On mode is completed the L2 cache, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs are accessible and coherent without requiring any software configuration.

**1/2 RAM ON**

In this PPU mode, the Cortex®-R82AE processor shared logic, L2 duplicate L1 tag RAMs, and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs are powered up but half of the L2 cache RAMs remain powered down.

**DL1ONLY ON**

In this PPU mode, the Cortex®-R82AE processor shared logic, L2 duplicate L1 tag RAMs, and LCU duplicate L1 tag RAMs are powered up but the L2 cache RAMs remain powered down.

## FULL RAM MEM\_RET, 1/2 RAM MEM\_RET

In this PPU mode, the L2 cache RAMs are in retention, but the rest of the Cortex®-R82AE processor shared logic is powered down, apart from the PPU. This is also known as Dormant mode. The L2 cache still contains data and if another agent in the system needs to snoop the cluster to access that data then the cluster needs to transition to an On mode before the snoop can proceed. As this transition takes a significant amount of time, Arm recommends that MEM\_RET is only used when other coherent agents are also idle.

## DL1ONLY MEM\_RET

In this PPU mode, the L2 cache RAMs are powered down and their content is not retained. Therefore this operating mode is equivalent to OFF mode. DL1ONLY MEM\_RET is provided for consistency so that a system can choose to go to the MEM\_RET state without needing to know the current operating mode.

## DL1ONLY MEM\_RET\_EMU, FULL RAM MEM\_RET\_EMU, 1/2 RAM MEM\_RET\_EMU

In this PPU mode, the cluster logic including the L2 cache RAMs, L2 duplicate L1 tag RAMs, LCU duplicate L1 tag RAMs remains powered.

Individual cluster power modes such as ON, OFF, OFF\_EMU, MEM\_RET\_EMU, DBG\_RECOV, and WARM\_RST are also considered to be PPU modes. See [5.9 Cluster power modes](#) on page 84 for more information on the description of these power modes.

### 5.11.1 Rules governing cluster PPU mode transitions

For the cluster *Power Policy Unit* (PPU) mode transitions, there is a set of rules that governs the transitions from each PPU mode. The PPU are aware of these rules, so there is no requirement for the *System Control Processor* (SCP) or a core within the Cortex®-R82AE processor through a Utility bus loopback connection to explicitly program these rules into the PPU.

The following rules govern all transitions between the PPU modes:

- When transitioning from OFF to ON, any supported operating mode can be targeted.
- Transitions between operating modes only happen in the ON power mode.
- Switching between DL1ONLY and FULL RAM ON can be direct or through ½ RAM ON.
- The operating mode is maintained when moving from ON to MEM\_RET power mode.

### 5.11.2 PPU mode transition behavior

Where there is a transition between the *Power Policy Unit* (PPU) modes, the Cortex®-R82AE processor cluster logic automatically performs a series of actions before accepting a new PPU mode.

The following table shows the allowed transitions between the cluster PPU modes and the associated actions.



**Note**

For each of the PPU mode transitions shown in the following table, additional actions (which are technology and implementation dependent) must be performed. These actions are carried out by partner implemented logic as part of the *Power Control State Machine (PCSM)*.

**Table 5-5: Cluster PPU transition behavior**

Start PPU mode	End PPU mode	Cortex®-R82AE processor behavior
OFF	MEM_RET	No functional change.
OFF / OFF_EMU	ON	The L2 cache, L2 duplicate L1 tag RAMs, and LLRAM Coherency Unit (LCU) duplicate L1 tag RAMs are initialized, and the cluster is brought into coherency with the rest of the system. Cluster System register fields (except the debug, trace, and RAS register fields) which reset to architecturally <b>UNKNOWN</b> values are initialized to fixed values.
OFF_EMU	OFF	No functional change.
OFF_EMU	MEM_RET_EMU	No functional change.
MEM_RET / MEM_RET_EMU	ON	The L2 duplicate L1 tag RAMs and LCU duplicate L1 tag RAMs are initialized. Cluster System register fields (except the debug, trace, and RAS register fields) which reset to architecturally <b>UNKNOWN</b> values are initialized to fixed values.
MEM_RET_EMU	MEM_RET	No functional change.
ON	OFF / OFF_EMU	If there is any ongoing memory access, the request is denied. L2 cache allocation disabled, L2 cache cleaned and invalidated. The cluster is removed from system coherency.
ON	MEM_RET / MEM_RET_EMU	If there is any ongoing memory access, the request is denied.
ON	WARM_RST	Cluster System registers (excluding the debug, trace, and RAS registers) are reset.
WARM_RST	ON	Relevant ways in L2 cache are invalidated. Cluster System register fields (except the debug, trace, and RAS register fields) which reset to architecturally <b>UNKNOWN</b> values are initialized to fixed values.
Any mode	DEBUG_RECOV	Transition accepted immediately. Warm reset or Cold reset is applied depending on the value of DBG_RECOV_PORST_EN
DEBUG_RECOV	ON	Reset is deasserted. MACP and ACELS interfaces are enabled.
DL1ONLY	½ RAM	L2 cache tag RAM ways 0-3 invalidated. Cache lookup and allocation enabled for ways 0-3.
DL1ONLY	FULL RAM	L2 cache tag RAM ways 0-7 invalidated. Cache lookup and allocation enabled for ways 0-7.
½ RAM	DL1ONLY	L2 cache tag RAM ways 0-3 allocation is prevented. Ways 0-3 are cleaned of any dirty lines and then cache lookup is disabled.
½ RAM	FULL RAM	L2 cache tag RAM ways 4-7 invalidated. Cache lookup and allocation enabled for ways 4-7.
FULL RAM	½ RAM	L2 cache tag RAM ways 4-7 allocation is prevented. Ways 4-7 are cleaned of any dirty lines and then cache lookup is disabled.

Start PPU mode	End PPU mode	Cortex®-R82AE processor behavior
FULL RAM	DL1ONLY	L2 cache tag RAM ways 0-7 allocation is prevented.  Ways 0-7 are cleaned of any dirty lines and then cache lookup is disabled.

### 5.11.3 DebugBlock power modes

The DebugBlock supports only two power modes, ON and OFF. There is no *Power Policy Unit* (PPU) in the Cortex®-R82AE processor for the DebugBlock. Instead, the DebugBlock has a Q-Channel interface for providing power control to the DebugBlock power domain.

When the DebugBlock is in the OFF mode, the DebugBlock does not initiate any accesses and all APB accesses to the DebugBlock receive a PSLVERR response.

## 5.12 Cluster powerdown

The cluster is taken out of coherency automatically when it is powered down. No software sequence is required.

After receiving the request to enter powerdown mode from the power controller, the Cortex®-R82AE processor cleans and invalidates the L2 cache and communicates with the interconnect to disable snoops into the cluster. All cores must be in the OFF mode before the cluster is powered down.



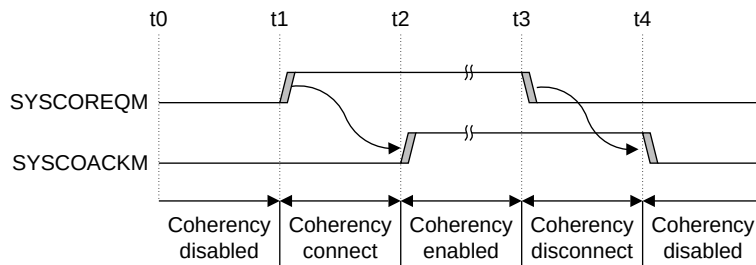
To support automated removal from coherency, the interconnect must support the SYSCOREQM and SYSOCOACKM handshake protocol. If not, the SoC is responsible for programming the interconnect to remove the cluster from coherency.

### 5.12.1 Transitioning in and out of coherency

The Cortex®-R82AE processor provides a hardware mechanism for taking the cluster in and out of coherence with the system interconnect. The cluster enables coherency during powerup and disables it during powerdown.

The system interconnect can use signals, SYSCOREQM, and SYSOCOACKM, to take the cluster in and out of coherence. If the system interconnect supports these signals, they can be connected directly. If the system interconnect does not support these signals, Arm recommends that they are connected to the power controller. In this case, the power controller must take any actions necessary to make the transition.

The following diagram shows the timing of SYSCOREQM, and SYSOCOACKM.

**Figure 5-5: SYSCOREQM SYSCOACKM four-phase coherency handshake**

During the memory retention (emulated) mode, SYSCOREQM will be held to be HIGH, so that the coherency can keep to enable. When the system interconnect has enabled coherency, it asserts SYSCOACKM and can then start sending snoop requests to the cluster. The cluster accepts snoop requests whenever either signal is asserted.

The cluster disables coherency during powerdown. The cluster deasserts SYSCOREQM, and waits for the system interconnect to deassert SYSCOACKM. The system interconnect must not deassert SYSCOACKM until it can guarantee that: there are no further snoop requests to be sent, and that all snoop requests it has already sent have fully completed.

The signals must obey the following four-phase handshake rules:

- SYSCOREQM can only change when SYSCOACKM is at the same level.
- SYSCOACKM can only change when SYSCOREQM is at the opposite level.

## 5.13 Cluster power mode and core power mode dependencies

There are some dependencies between the core and cluster power domains to ensure that correct operation is maintained.

The core and cluster power mode dependencies are the following:

- If a core ON request is made while the cluster is not in an ON mode, then the core request stalls until the cluster has reached the appropriate state.
- If a core is requested to go from WARM\_RST to ON, the core request stalls until the cluster has transitioned from WARM\_RST to ON.
- If a core is requested to go from DBG\_RECOV to ON, the core request stalls until the cluster has transitioned from DBG\_RECOV to ON.
- If the cluster is requested to go to MEM\_RET or OFF while not all cores are OFF, then the cluster request is denied.
- If the cluster is requested to go from WARM\_RST to ON, the cluster request is denied unless all the cores are in OFF, OFF\_EMU, or WARM\_RST.

- If the cluster is requested to go from DBG\_RECOV to ON, the cluster request is denied unless all the cores are in OFF, OFF\_EMU, or DBG\_RECOV.
- If the cluster is requested to go to MEM\_RET\_EMU or OFF\_EMU while not all cores are OFF or OFF\_EMU, then the cluster request is denied.

## 6. Power and reset control with PPU

This chapter describes how to control the power modes and reset behavior of the Cortex®-R82AE processor by using the *Power Policy Units* (PPUs).

### 6.1 The Power Policy Unit

The *Power Policy Units* (PPUs) enable control over the power modes of the Cortex®-R82AE processor. The cluster PPU allows control over the cluster power and operating modes. Per-core PPU allows control over the individual core power modes.

A PPU is a standard component for abstracting the low-level hardware control signaling to software-controlled power domain policy. This allows the external agent to focus on the power modes it wants to achieve without being concerned about the intermediate power modes.

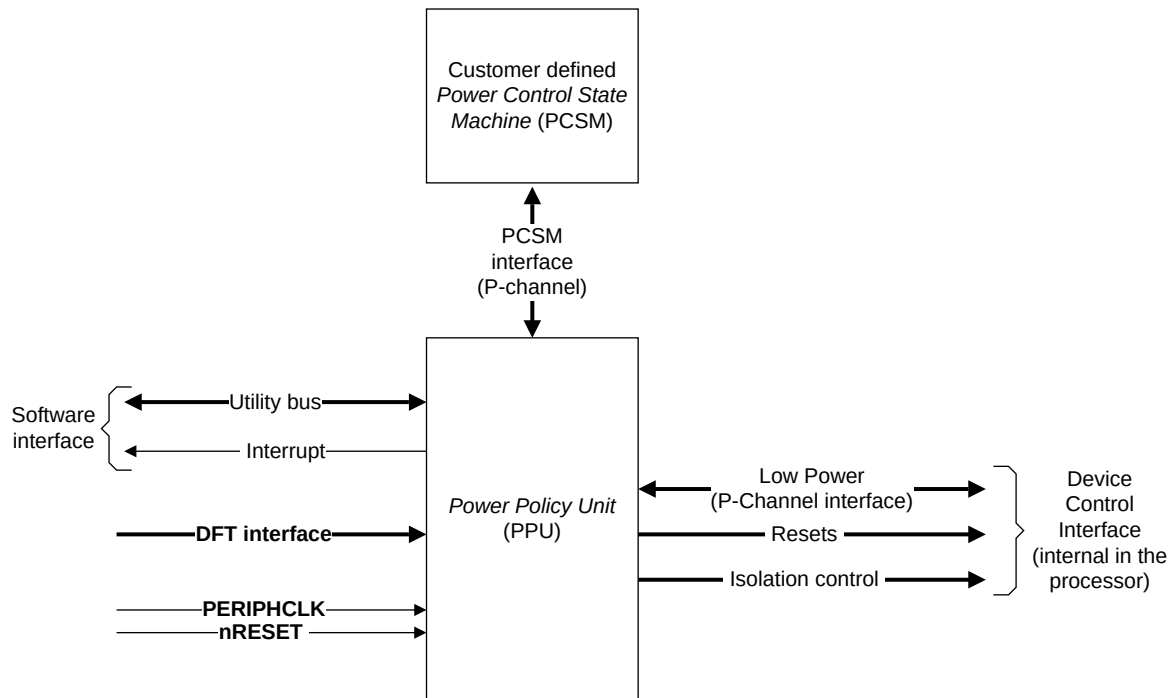
The implementation process automatically creates the PPU for the cluster and each core. Each PPU has a set of memory-mapped control registers which are accessed using the Utility bus.

The PPU can provide autonomous control of power modes with a range of modes. A component in the system such as a *System Control Processor* (SCP) can program the PPU over the Utility bus to set the appropriate power policy.

If your system does not have an SCP component, the Utility bus can be connected to one of the Cortex®-R82AE processor ports or to your SoC interconnect, and one of the cores within the Cortex®-R82AE processor can program the PPU. For information on the loopback address mapping through the interconnect, see [8.11 Utility bus](#) on page 195. For information on potential limitations of not using an SCP or not implementing a Utility bus loopback connection, see [6.9 Implications of not having a System Control Processor](#) on page 110.

The PPU controls the low-level details of powering up, powering down, or resetting domains as necessary to implement the requested policy. The hardware performs any actions necessary to reach the requested power mode, such as gating clocks, flushing caches, or disabling coherency.

The following figure shows the Cortex®-R82AE processor PPU interfaces. All interfaces are external to the Cortex®-R82AE processor apart from the Device Control interface.

**Figure 6-1: PPU interfaces**

The cluster PPU and per-core PPUs have the following main interfaces:

### Software interface

The programming interface for the PPUs is accessed through the Utility bus. A set of PPU registers controls setting high-level policy control and configuration.

### Device Control interface

The Device Control interface is the internal interface that connects to each of the cluster and core power domains. The Device Control interface provides low-level power control and ensures device quiescence.

The Device Control interface includes:

- The device interface that consists of one or more P-Channels.
- The control interface that includes resets and isolation control.



**Note**

Some of the Device Control interface signals are exported outside of the Cortex®-R82AE processor to allow the control of other components that may be in the same power domain.

### PCSM interface

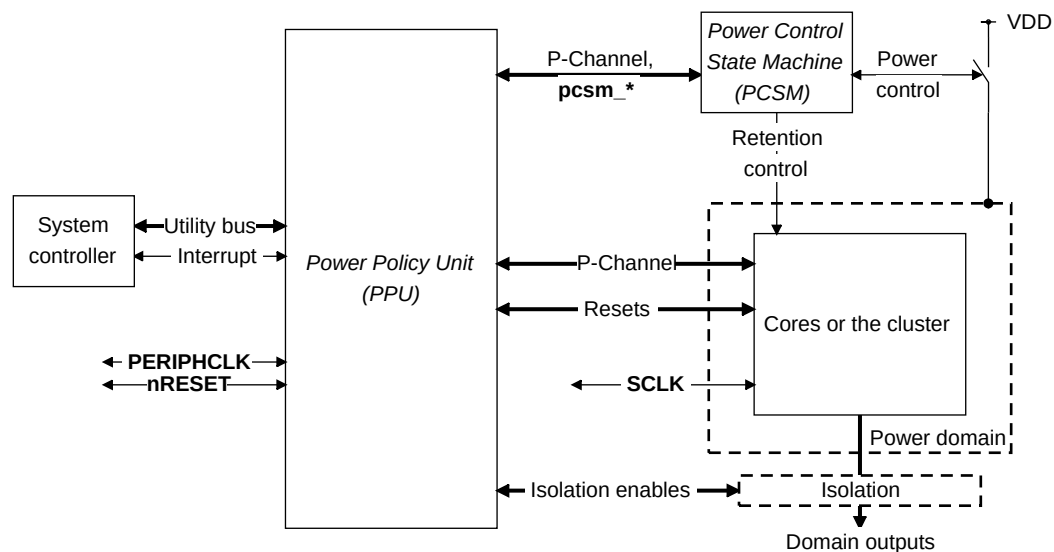
The *Power Control State Machine* (PCSM) interface is an external interface for controlling low-level technology specific power switch and retention controls. There are separate PCSM interfaces for the cluster and each core instantiated in the Cortex®-R82AE processor.

**Note**

The PCSM interface is always present even if your system does not implement some Cortex®-R82AE power domains for cluster or core. For information on how to connect P-Channel signals in such cases, see P-Channel signals in *Arm® Cortex®-R82AE Configuration and Integration Manual*.

The following figure shows a high-level illustration of how the PPU and PCSM controls connect to each other and to a power-gated domain. The dotted lines indicate the implementation-dependent components and signal connections.

**Figure 6-2: PPU connections to a power-gated domain**



All the PPUs within the Cortex®-R82AE processor are pre-built and are based on the CoreLink PCK600 Power Policy Units.

**Note**

The CoreLink PCK600 does not require a separate license. It is delivered as part of the Cortex®-R82AE processor.

## 6.2 PPU operation

The *Power Policy Unit* (PPU) controls all of the Cortex®-R82AE processor cluster and core power modes (ON, OFF, OFF\_EMU, FUNC\_RET, FULL\_RET, MEM\_RET, MEM\_RET\_EMU, WARM\_RST, and DBG\_RECOV). It has extensive support to reflect the various combinations of logic and memory power states into which a domain can be set.

Your software can program a PPU to set a PPU mode in one of two ways:

### Static policy

A request to enter a PPU mode directly.

### Dynamic policy

Sets a minimum mode, so the PPU can autonomously change the PPU mode above this mode depending on hardware inputs.

Each PPU contains a state machine representation of its supported PPU mode transitions. Therefore, a PPU can be programmed to target any supported PPU mode and the route taken follows the permissible route, passing through any intermediate PPU modes.

Each of the PPU has an interrupt output signal that indicates events such as the completion of power mode transitions and the completion of operating mode transitions. For the cluster, this is CLUSTERPPUIRQ and for the cores these are COREPPUIRQ[<m>], where <m> is the core instance number. These interrupts can be targeted to the agent which programs the PPU to avoid polling status registers.

A *System Control Processor* (SCP) or a core in the Cortex®-R82AE processor programs the PPU through the Utility bus based on its current system requirements. The PPU modes are programmed using registers within the PPU. When a PPU mode is programmed into the PPU registers, this PPU mode is requested internally within the Cortex®-R82AE cluster. The relevant cluster logic takes the necessary steps to enter this mode such as cleaning dirty cache lines from the caches when powering off. When the logic is ready to enter the required mode, the change in power state is requested on the relevant *Power Control State Machine* (PCSM) interface. When the power state transition is complete, the PCSM is responsible for changing the power state for the relevant logic and signaling to the PPU.

If the relevant logic is required to be isolated or removed from isolation this is signaled using the relevant ISOLATE signals (CLUSTERISOLATE<sub>n</sub>, L2RAMISOLATE<sub>n</sub>, FPSIMDISOLATE<sub>n</sub>, and COREISOLATE<sub>n</sub>). As the isolation signals do not have an acknowledge signal, the state of the isolation cells is changed at a software-dependent time later after a change of the ISOLATE signals. The latency time on the ISOLATE signal change can be configured by PPU registers. The PPU logic ensures that the isolation and power state change are requested in the required order for the requested PPU mode transition.

### 6.2.1 Implicit resets from PPU mode change

Transitions between power down modes and powered modes include an implicit internal reset of the powered off logic. This internal reset is managed by the *Power Policy Unit* (PPU) mode



controlling the transition between the two modes and does not require an external signal to be asserted or explicit programming of the PPU.

A transition from an Off mode to a power mode includes a Cold reset of the logic that was powered off, where both functional logic and debug logic is reset.

A transition from an Emulated off mode to a power mode includes a Warm reset of the logic that was emulated as powered off, where the functional logic is reset but the Debug, Trace and *Reliability, Availability, and Serviceability* (RAS) state is not reset.

## 6.3 Utility bus accesses

All of the *Power Policy Unit* (PPU) control and data registers are accessed using the memory mapped Utility bus. The Utility bus is implemented as a 64-bit AMBA® 5 AXI subordinate port.

Accesses to PPU registers over the Utility bus must match the size of the register they are accessing, either 32 bits or 64 bits. Any access with sizes other than 32-bit or 64-bit gets an SLVERR response from the Utility bus.

Cores within the Cortex®-R82AE processor cannot access to the PPU registers directly. Instead, you must either use a *System Control Processor* (SCP), or configure your interconnect to provide a loopback address mapping for the cores to access the Utility bus. See [6.9 Implications of not having a System Control Processor](#) on page 110 for information on how to program the PPU from within the Cortex®-R82AE processor.

The registers for the cluster PPU and each of the core PPU are grouped on separate 64KB page boundaries allowing access control to be enforced by the memory management. The DESNSE\_CS\_ADDR\_MAP options allows for packing for 4KB page boundaries.

Only secure accesses are allowed on the Utility bus to access PPU registers. Any Non-secure access gets an SLVERR response from the Utility bus.

## 6.4 Encodings for cluster power modes and operating modes

The cluster *Power Policy Unit* (PPU) power policy register CLUSTERPPU\_PWPR uses power mode and operating mode encodings to set various power conditions for the cluster. For example, the values at the register bitfields CLUSTERPPU\_PWPR.PWR\_POLICY and CLUSTERPPU\_PWPR.OP\_POLICY set the power mode and operating mode of the cluster.

The following table shows the Cortex®-R82AE processor cluster level power mode encodings.



Note

- Priority is an architectural concept as defined in [Arm® Power Policy Unit Architecture Specification](#).
- INPUTDOMAINPSTATE[3:0] and OUTPUTDOMAINPSTATE[3:0] encodings are the same as the CLUSTERPPU\_PWPR.PWR\_POLICY[3:0] encodings.

**Table 6-1: Power mode enumeration for the cluster**

Power mode	CLUSTERPPU_PWPR.PWR_POLICY[3:0]	CLUSTERPCSMPSTATE[3:0]	CLUSTERPPUHWSTAT[15:0]	Priority
OFF	0x0	0x0	0x0001	Low
OFF_EMU	0x1	0x8	0x0002	-
MEM_RET	0x2	0x2	0x0004	-
MEM_RET_EMU	0x3	0x8	0x0008	-
ON	0x8	0x8	0x0100	-
WARM_RST	0x9	0x8	0x0200	-
DBG_RECOV	0xA	0x8	0x0400	High

The following table shows the Cortex®-R82AE processor cluster operating mode encodings for CLUSTERPCSMPSTATE[5:4] and CLUSTERPPUHWSTAT[23:16].

**Table 6-2: Operating mode enumeration for the cluster**

Operating mode	Short name	CLUSTERPPU_PWPR.OP_POLICY	CLUSTERPCSMPSTATE[5:4]	CLUSTERPPUHWSTAT[23:16]	Priority
L2 duplicate L1 tag RAM and LLRAM Coherency Unit (LCU) duplicate L1 tag RAM only	DL1ONLY	0x0	0x0	0x01	Low
Half L2 cache	½ RAM	0x1	0x1	0x02	Medium
Full L2 cache	FULL RAM	0x2	0x2	0x04	High

For information on these registers, see [Arm® Power Policy Unit Architecture Specification](#).

## 6.5 Encodings for core power modes

The core *Power Policy Unit* (PPU) power policy registers PPU\_PWPR use power mode encodings to set various power modes for the cores.

The following table shows the power mode encodings for the cores in the Cortex®-R82AE processor.

**Note**

In the following table <m> is the core instance number and Priority is an architectural concept as defined in [Arm® Power Policy Unit Architecture Specification](#).

**Table 6-3: Power mode enumeration for the cores**

Power mode	PPU_PWPR.PWR_POLICY	CORE<m>PCSMSTATE[3:0]	CORE<m>PPUHWSTAT[15:0]	Priority
OFF	0x0	0x0	0x0001	Low
OFF_EMU	0x1	0x8	0x0002	-
FULL_RET	0x5	0x5	0x0020	-
FUNC_RET	0x6	0x7	0x0080	-
ON	0x8	0x8	0x0100	-
WARM_RST	0x9	0x8	0x0200	-
DBG_RECOV	0xA	0x8	0x0400	High

## 6.6 Programming sequences for the cluster and the core

Each request for a change in *Power Policy Unit* (PPU) mode triggers a power state request on the *Power Control State Machine* (PCSM) interface for the respective core or cluster. The PCSM must accept the change request in power state before the PPU mode can change.

A request on the PCSM interface can be accepted automatically for designs where:

- There is no active power management at all.
- The cluster is being analyzed in a non-power aware environment.

### 6.6.1 Programming sequence to bring the cluster and cores from Off to On mode

Use the following steps to program the *Power Policy Unit* (PPU) for the cluster and each core to request a change in PPU mode from Off to On.

#### About this task

This task uses the PPU static policy to request a single mode transition. <m> is the core instance number.

#### Procedure

1. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the cluster register CLUSTERPPU\_PWPR, address 0x010000, value 0x00020008.

This sets the power mode policy to ON and the operating mode policy to FULL RAM.

2. Poll the cluster CLUSTERPPU\_PWSR register, address 0x010008, until the value read matches the value written to the PPU\_PWPR register.  
Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the cluster CLUSTERPPU\_PWSR register.



Any update to cluster or core PPU registers, including the PPU Interrupt Mask Register, requires a write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA.

The *Power Control State Machine* (PCSM) for the cluster must respond back to the PPU mode request before the mode is accepted.

3. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the core PPU\_PWPR register, for core <m>, address 0x<m>40000, value 0x00000008.
4. Poll the core PPU\_PWSR register for core <m>, address 0x<m>40008, until the value read matches the value written to the PPU\_PWPR register.  
Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the core PPU\_PWSR register.

Each core PCSM must respond back to the PPU mode request before the mode is accepted.

## 6.6.2 Programming sequence to bring the cluster and cores from On to Off mode

Use the following steps to program the *Power Policy Unit* (PPU) for the cluster and each core to request a change in PPU mode from On to Off.

### About this task

This task uses the PPU static policy to request a single mode transition. <m> is the core instance number.

### Procedure

1. Software running on the core sets the IMP\_CPUPWRCTLR\_EL1.PWRDN bit to 1, then executes a WFI instruction. For the full sequence see, [5.8 Core powerdown](#) on page 83.
2. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the core PPU\_PWPR for core <m>, address 0x<m>40000, value 0x00000000.
3. Poll the core PPU\_PWSR register for core <m>, address 0x<m>40008, until the value read matches the value written to the PPU\_PWPR register.  
Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the core PPU\_PWSR register.

The core *Power Control State Machine* (PCSM) must respond back to the PPU mode request before the mode is accepted.

4. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the cluster CLUSTERPPU\_PWPR register, address 0x010000, value 0x00000000.
5. Poll the cluster CLUSTERPPU\_PWSR register, address 0x010008, until the value read matches the value written to the CLUSTERPPU\_PWPR register.  
Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the cluster CLUSTERPPU\_PWSR register.

The cluster PCSM must respond back to the PPU mode request before the mode is accepted.

### 6.6.3 Programming sequence for an interrupt controller to bring cores and cluster to On or Off mode

The following sequence makes it possible for the cluster and cores in the Cortex®-R82AE processor to automatically power down when software running on the processor has nothing more to do. It also enables the cluster and cores to automatically power up when they receive the asserted signal COREWAKEREQUEST[<m>] from an interrupt controller.

#### About this task

This task uses the PPU dynamic policy to request automatic transitions. <m> is the core instance number.

#### Procedure

1. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the cluster CLUSTERPPU\_PWPR register, address 0x010000, value 0x01000100.
2. Write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA. Write to the core PPU\_PWPR for core <m>, address 0x<m>40000, value 0x00000100.
3. To power up core <m> or power down core <m>, see the following steps.

##### Choice

To power up core <m>

To power down core <m>

##### Step

Assert the COREWAKEREQUEST[<m>] signal.

Software on the core sets the IMP\_CPUPWRCTLR\_EL1.PWRDN bit to 1, then executes a WFI instruction. The full power down sequence in [5.8 Core powerdown](#) on page 83 should be respected.

When all cores are powered off, the cluster will power off with no additional action needed.



Note

The signal COREWAKEREQUEST[<m>] is level sensitive.

## 6.7 Explicit resetting of cluster and cores and debug recovery

You can reset part or all of the Cortex®-R82AE processor in various ways. This section describes the sequences to reset part or all of the Cortex®-R82AE processor.



Note

- You must follow the sequences exactly.
- The *Power Policy Units* (PPUs) and associated logic prevents unsupported transactions from occurring.
- The examples that refer to addresses of PPU registers, assume that the parameter `DENSE_CS_ADDR_MAP = 0`
- The `WARM_RST` and `DBG_RECOV` power modes do not have an associated operating mode. Therefore before entering these power modes, the current cluster operating mode must be saved. This ensures that the same operating mode can be restored when leaving the power states.

### Powerup (Cold) reset

This reset must be done the first time that the cluster is powered up. It resets all the Cortex®-R82AE processor including the PPU.



Note

This procedure can be achieved by either programming the PPU over the Utility bus or configuring the `PPU_RST_STATE` parameter to 1.

1. Assert the `nRESET` signal for a minimum of 10 or more `PERIPHCLK` cycles.
2. Deassert the `nRESET` signal.
3. Program the PPU for the cluster to On mode, see [6.6.1 Programming sequence to bring the cluster and cores from Off to On mode](#) on page 103.
4. Program the PPU for each core to On mode, see [6.6.1 Programming sequence to bring the cluster and cores from Off to On mode](#) on page 103.



Note

Steps 3 and 4 are not needed if the Cortex®-R82AE processor is configured with `PPU_RST_STATE = 1`. See [6.9 Implications of not having a System Control Processor](#) on page 110 for more information.

## Software initiated Warm reset of an individual core



Note

- This procedure does not require any access on the Utility bus.
- Interrupts and other external accesses are expected to be redirected or paused from the point this procedure is initiated until the core restarts execution.

1. Use software running on the core to program the RMR\_EL2.RR register bit.
2. Execute a `WFI` instruction.

## Software initiated Cold or Warm reset of the cluster (excluding the PPUs)

For the Cold reset case, power is also removed from the cluster during this sequence.



Note

This procedure requires an external SCP connected via the Utility bus.

1. Use software running on each core to set the IMP\_CPUPWRCTLR\_EL1.PWRDN bit.
2. Use software running on each core to execute a `WFI` instruction.
3. Program the core's PPU, and then the cluster PPU, to Off mode (Cold reset) or Emulated off mode (Warm reset) as per [6.6.2 Programming sequence to bring the cluster and cores from On to Off mode](#) on page 104.



Note

- The cluster Off mode can only be entered if all the cores are in Off mode.
- To use Emulated off in the cluster, core, or both a value of `0x00000001` should be written to CLUSTERPPU\_PWPR and PPU\_PWPR respectively.

4. To transition from Emulated off mode back to On, first program the cluster PPU to ON. Then program the Core PPUs to ON.
5. To transition from Off mode to On mode, see [6.6.1 Programming sequence to bring the cluster and cores from Off to On mode](#) on page 103.

## Using WARM\_RST mode to reset the cluster (excluding the PPUs)

This procedure can be used to recover from a watchdog timeout or similar situations.



Note

This procedure can be achieved by the *System Control Processor* (SCP) over the Utility bus. If your system does not have an SCP, you have to enable an external agent such as debugger that has memory mapped access to the Utility bus.

1. Ensure that the cluster is in On mode and the cores are either in On mode, Off mode, or Emulated off mode. Read the PPU\_PWSR for the cluster to determine the current cluster operating mode.

**Note**

Before every register write, the user must first write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA.

2. For any of the cores that are in On mode, write to the core PPU\_PWPR for core <n>, address 0x<n>40000, value 0x00000009. This sets the core to the WARM\_RST power mode.
3. Write to the cluster PPU\_PWPR, address 0x010000, value 0x00000009. This sets the cluster to the WARM\_RST power mode.
4. Write to the cluster PPU\_PWPR, address 0x010000, value 0x000<p>0008, where <p> is the operating mode value read in step 1. This sets the cluster to the ON power mode.
5. For each core that is in WARM\_RST, write to the core PPU\_PWPR register, for core <n>, address 0x<n>40000, value 0x00000008. This puts each core back to the ON power mode.

**Note**

After each of the \*PPU\_PWPR is configured, the corresponding \*PPU\_PWSR should be polled until the value read matches the value written to the \*PPU\_PWPR register. Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the cluster \*PPU\_PWSR register. Addresses for these can be found in [B.1.2.2.3 PPU\\_PWSR, Power Status Register](#) on page 1569. The corresponding PCSM must respond back to the PPU mode request before the mode is accepted.

### Reset of the cluster (excluding the PPU), retaining cache contents for debug

This can be either a Warm reset or Cold reset, depending on the setting of the PPU\_PTCR.DBG\_RECOV\_PORST\_EN bit.

**Note**

This procedure can be achieved by the *System Control Processor* (SCP) over the Utility bus. If your system does not have an SCP, you have to enable an external agent such as debugger that has memory mapped access to the Utility bus.

**Note**

The value in PPU\_PTCR.DBG\_RECOV\_PORST\_EN bit must be the same for all PPU (the cluster and all the cores). Otherwise the results are **UNPREDICTABLE**.

1. Read the PPU\_PWSR for the cluster and each core to determine which cores are powered up and what is the current cluster operating mode.



2. For any cores that are already OFF, you must ensure they are in a static OFF, or in a LOCKED OFF (PPU\_PWPR.LOCK\_EN = 1 for core <m>, address 0x<m>40000, bit 12) state to ensure they do not power up during this process.
3. Check the cluster operating mode and ensure it is in a static configuration so that the operating mode does not change after this step.

**Note**

Before every register write, the user must first write to the cluster safety write key register CLUSTERSAFETY\_WRITEKEY, address 0x080060, value 0x000000BA.

4. Write to the core PPU\_PWPR for core <m>, address 0x<n>40000, value 0x0000000A. This sets the core to the DBG\_RECOV power mode.
  - If PPU\_PTCR.DBG\_RECOV\_PORST\_EN = 1, any core not in the OFF mode must be put in the DBG\_RECOV mode.
  - If PPU\_PTCR.DBG\_RECOV\_PORST\_EN = 0, any core not in the OFF or OFF\_EMU mode must be put in the DBG\_RECOV mode.
5. Write to the cluster PPU\_PWPR, address 0x010000, value 0x0000000A. This sets the cluster to the DBG\_RECOV power mode.
6. Write to the cluster PPU\_PWPR, address 0x010000, value 0x000<p>0008, where <p> is the operating mode value read in step 1. This sets the cluster to the ON power mode.
7. For each core that is in DBG\_RECOV, write to the core PPU\_PWPR register, for core <m>, address 0x<n>40000, value 0x00000008. This sets each core back to the ON power mode.

- After each of the \*PPU\_PWPR is configured, the corresponding \*PPU\_PWSR should be polled until the value read matches the value written to the \*PPU\_PWPR register. Alternatively, you can enable the PPU interrupt and wait for the interrupt from the PPU to read the cluster \*PPU\_PWSR register. Addresses for these can be found in [B.1.2.2.3 PPU\\_PWSR, Power Status Register](#) on page 1569. The corresponding PCSM must respond back to the PPU mode request before the mode is accepted.

**Note**

- If your system does not have a *System Control Processor* (SCP), some of the sequences above might not be available. For information on potential limitations of not using an SCP or not implementing a Utility bus loopback connection, see [6.9 Implications of not having a System Control Processor](#) on page 110.
- To control transitions through in and out of DBG\_RECOV and WARM\_RST power modes, it is expected that a debugger will have memory mapped access to the Utility bus. Therefore, even if your system does not have an SCP, it should provide memory mapped access to the Utility bus for debug control.

## 6.8 ECC errors during power transitions

It is possible to get *Error Correcting Code* (ECC) errors in the RAMs during a power transition. These ECC errors could happen during the software sequence shortly before the hardware sequence starts. Alternatively, these ECC errors could happen during the hardware sequence when the L1 or L2 cache is cleaned and invalidated as part of the On to Off power mode transition for a core or the cluster.

If the *Reliability, Availability, and Serviceability* (RAS) interrupts are enabled and if RAS errors occur which cause RAS interrupts while the cluster is powering down, then the RAS interrupts prevent the core or the cluster from powering down to prevent loss of information.

The RAS interrupts can be disabled. If the RAS interrupts are disabled, then even though a RAS error occurs during a power down transition, the core or cluster can still continue with the powering down.

If the RAS interrupts are enabled, then you must ensure that your system has either of the following:

- An external system level error manager which has the ability to read and write RAS records through the Utility bus.
- Nominated one (or more) Cortex®-R82AE processor core to be responsible for handling the RAS interrupts. In this case, the nominated core and the cluster must be always powered on and available to handle the RAS interrupts. The nominated core must also have access to the RAS records through a Utility bus loopback.



In systems where the RAS interrupts are enabled, if there is no external system level error manager and if the nominated core for handling the RAS interrupts is powered down, this can lead to an incomplete state. This is because a denied power transaction will leave the nominated core powered on but stuck in WFI. In this case, the RAS interrupts will remain active but not be serviced.

---

Although the ECC errors are reported in the RAS error record registers, once the cluster or core is powered down, the RAS registers are no longer accessible. If the RAS registers are reporting an error and the RAS interrupts are enabled, the following sequence happens:

1. The RAS interrupt signals (nCOREERRIRQ, nCOMPLEXERRIRQ, nCOREFAULTIRQ, nCOMPLEXFAULTIRQ or nCOMPLEXCRITIRQ) for the appropriate core or cluster are asserted.
2. If the *Power Policy Unit* (PPU) is requesting a transition to an OFF power mode, then the request to OFF power mode is denied.
3. The error interrupts must be sent to either an external system level error manager or a nominated Cortex®-R82AE processor core which is always on. The external system level error manager or a nominated core then reads and writes the relevant RAS error record registers through the Utility bus in order to clear the record of the reported fault or error. Once the error record has been cleared, the PPU will be able to request the OFF power mode again.

## 6.9 Implications of not having a System Control Processor

The global `PPU_RST_STATE` parameter defines the Cold reset state for the core and cluster *Power Policy Units* (PPUs).

`PPU_RST_STATE` supports the following values:

- 0** Cluster PPU and all core PPUs reset to Off.
- 1** Cluster PPU and all core PPUs reset to On.

Setting the `PPU_RST_STATE` to 0 ensures the whole Cortex®-R82AE processor is Off until a *System Control Processor* (SCP) powers it On. You must use this option only if your system includes an SCP that is connected to the Cortex®-R82AE processor Utility bus.

Setting the `PPU_RST_STATE` to 1 allows all the PPUs to transition from Off to On automatically after reset deassertion, without any programming by the SCP. If required, any core within the Cortex®-R82AE processor can still access the PPUs through the *Main Manager* (MM) port or the *Shared Peripheral Port* (SPP) that is connected via a loopback to the Utility bus. For an example of a loopback address mapping, see [8.11 Utility bus](#) on page 195.

You must consider the following when configuring the `PPU_RST_STATE`:

- If your system has an SCP, `PPU_RST_STATE` can be configured to either 0 or 1.
- If your system does not have an SCP, configure the `PPU_RST_STATE` to 1. Configuring the `PPU_RST_STATE` to 0 will leave your Cortex®-R82AE cluster permanently to an Off state, if no agent is able to program the PPUs.

If your system does not have an SCP or a loopback connection to the Utility bus, there is no way to program the PPUs. This means several things such as dynamic OPMODE transitions will not work. Also, some of the sequences in [6.7 Explicit resetting of cluster and cores and debug recovery](#) on page 105 cannot happen. For some of those cases you have to enable an external agent such as debugger that is connected to the Utility bus in your system to enable the cluster and cores to On mode to avoid a system deadlock.

## 6.10 PPU and reset management register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary tables for the core and cluster *Power Policy Unit* (PPU) registers in [B.1.1.2 External PPU registers summary](#) on page 1499 and [B.1.1.3 External CLUSTERPPU registers summary](#) on page 1501.

## 7. Initialization

This chapter describes considerations for initializing the Cortex®-R82AE processor.

### 7.1 Initializing the Cortex®-R82AE processor

You need to consider several things before you can run any program on the Cortex®-R82AE processor. This includes, initializing all programmer-visible registers, enabling the *Memory Protection Unit* (MPU), enabling the *Floating Point Unit* (FPU), invalidating the caches, and programming the *Power Policy Units* (PPUs).

#### Initializing the registers

Most of the architectural registers in the Cortex®-R82AE processor, such as X0-X30 and S0-S31 and D0-D31 when Advanced SIMD is included, do not have an architecturally defined reset value, that is they have an **UNKNOWN** value after reset. The Cortex®-R82AE processor includes hardware that automatically initializes all programmer-visible registers to a fixed value out of reset, including those which do not have an architecturally defined reset value.



The *Process State* (PSTATE) and some System register fields are given a known value on reset, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

---

Each core within the Cortex®-R82AE processor includes hardware that initializes all core programmable-visible registers after a core reset, unless the reset is for debug recovery.

Similarly, the Cortex®-R82AE processor includes hardware that initializes all cluster programmer-visible registers after a cluster reset, unless the reset is for debug recovery.



You must not assume that these initialization values can be depended on. The initialization values must still be considered as **UNKNOWN**, and that they could change in subsequent processor releases. This means that software must always initialize the programmer-visible registers that are defined as having **UNKNOWN** reset values before using them.

---

In addition, before you run an application, remember to:

- Program particular values into various registers, for example, Stack Pointers.
- Enable various features, for example, error reporting.
- Enable Region Registers controlling *Data Tightly Coupled Memory* (DTCM), *Tightly Coupled Memory* (ITCM), *Low-latency Peripheral Port* (LLPP), and *Low-latency RAM* (LLRAM) regions.
- Program particular values into memory, for example, the TCMs.

## Enabling the MPU

To make use of the programmable regions in the *Memory Protection Unit* (MPU), you must configure and enable any regions you wish to use. The Cortex®-R82AE processor supports direct programming through System register operations.

Before you can use the programmable regions, you must:

- Program the required regions for your memory map
- Enable the programmed regions
- Enable translation in the *System Control Register* (SCTLR), SCTLR\_EL1.M and SCTLR\_EL2.M

If using programmable regions the MPU should not be enabled until the regions are programmed and active. It is also possible to make use of default attributes without enabling any programmable regions. Please refer to the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more details.

## Enabling the MMU

To use *Memory Management Unit* (MMU) at EL1/0 you must:

- Configure the pagetables in the memory
- Configure the TTBR register to point to the pagetables
- Configure the VTCR\_EL2.MSA bit to select VMSA in EL1/0
- Configure the HCR\_EL2 if virtualization needs to be enabled
- Enable the *System Control Register* (SCTLR) SCTLR\_EL1.M

## Enabling the FPU

You must enable the *Floating Point Unit* (FPU) before floating-point or Advanced SIMD instructions can be executed.

Enable the FPU as follows:

- Enable access to the FPU in the *Architectural Feature Access Control Register* (CPACR\_EL1) by setting the FPEN field.
- Disable trapping of FPU instructions in the *Architectural Feature Trap Register* (CPTR\_EL2) by resetting the TFP bit.

## Invalidating the caches

The Cortex®-R82AE processor L1 instruction and L1 data caches and, if implemented, L2 cache are automatically invalidated after a reset.

This operation can never report any ECC errors.



Each core within the Cortex®-R82AE processor includes hardware that invalidates all core caches after a core reset, only if the reset is not because of an MBIST request or for debug recovery and the core power mode transitions from any OFF mode to any ON mode.

Similarly, the Cortex®-R82AE processor includes hardware that invalidates the L2 cache, L2 duplicate L1 tag RAMs, and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs after a cluster reset, only if the reset is not because of an MBIST request or for debug recovery and the cluster power mode transitions from:

- Any OFF mode to any ON mode
- DL1ONLY ON to ½ RAM ON
- ½ RAM ON to FULL RAM ON

---

## Programming the PPU

The PPUs control the power modes and reset behavior of the Cortex®-R82AE processor.

You can control the cluster and core PPUs to reset to off or on with the global `PPU_RST_STATE` parameter. Depending on the value of the `PPU_RST_STATE` parameter, an external *System Control Processor* (SCP) or core 0 within the Cortex®-R82AE processor programs the PPUs through the Utility bus and brings the Cortex®-R82AE processor out of reset.

For more information on `PPU_RST_STATE` parameter, see [6.9 Implications of not having a System Control Processor](#) on page 110. For more information on the PPU programming sequences, see [6.6 Programming sequences for the cluster and the core](#) on page 103.

## 7.2 Initializing TCMs

Each core within the Cortex®-R82AE processor has two optional *Tightly Coupled Memories* (TCMs): an *Instruction Tightly Coupled Memory* (ITCM) and a *Data Tightly Coupled Memory* (DTCM).

You can configure the Cortex®-R82AE processor to:

- Enable the ITCM out of reset.
- Boot out of an initialized ITCM.

A core's TCMs can be initialized by that core directly or by an external agent. If an external agent is used, the Cortex®-R82AE processor supports enabling initialization of a core's TCMs before that core completes its reset exception sequence and setting the reset vector address to point into the initialized ITCM.



**Note**

Before initializing the TCMs, ensure that both `PDCLUSTER` and `PD<CPU>` power domains are ON, either by configuring the processor with `PPU_RST_STATE = 1` or by programming the *Power Policy Units* (PPUs).

---

## 7.2.1 Preloading TCMs

You can write data to the *Tightly Coupled Memories* (TCMs) by using either store instructions or the *ACE-Lite Subordinate* (ACELS) interface.

Depending on the method you choose, you might require:

- Particular hardware on the SoC that you are using, such as a DMA engine.
- Boot code.
- A debugger connected to the processor.

The methods to preload the TCMs include:

### Memory copy with running boot code

The boot code includes a memory copy routine that reads data from an external memory, and writes it into the appropriate TCM. You must enable the TCM to do this.

### Copy data from the Debug Communications Channel

The boot code includes a routine to read data from the *Debug Communications Channel* (DCC) and write it into the TCM. The debug host feeds the data for this operation into the DCC by writing to the appropriate registers on the processor APB debug interface.

### Execute code in debug halt state

The debug host puts the Cortex®-R82AE processor into debug halt state and then feeds instructions into it through the *External Debug Instruction Transfer Register* (EDITR). The Cortex®-R82AE processor executes these instructions, as an alternative to using boot code in either of the two methods previously described.

### DMA into TCM

The SoC includes a DMA device that reads data from a ROM and writes it to the TCMs through the ACELS interface.

## 7.2.2 Preloading TCMs with ECC

Before a RAM location is read with *Error Correcting Code* (ECC) protection enabled, the error code bits must be initialized.

The error code bits in the TCM RAM are not initialized by the Cortex®-R82AE processor.

The Cortex®-R82AE processor has separate controls of whether ECC checking is enabled and whether detected ECC errors are recorded and reported to the appropriate *Reliability, Availability, and Serviceability* (RAS) registers. For more information on the relevant registers see the MEMPROTEN fields in [A.2.2.48 IMP\\_MEMPROTCTLR\\_EL1, Memory Protection Control Register](#) on page 567 and [A.2.2.62 IMP\\_CLUSTERMEMPROTCTLR\\_EL1, Cluster Memory Protection Control Register](#) on page 615 and ED field in [B.1.2.1.2 ERR<n>CTLR, Error Record <n> Control Register, n = 0 - 9](#) on page 1507.

To update a TCM location without detecting an error, either the ECC checking or RAS reporting must be disabled or the write must be of the same width and aligned to the data chunk that the error scheme protects as described in this section.



Note

The reset value of IMP\_MEMPROTCTLR\_EL1.MEMPROTEN takes the value of the top-level pin CFGRAMPROTEN and the reset value of ERR<n>CTLR.ED is 0. If CFGRAMPROTEN is set to LOW, it implies that errors are not detected and are not recorded to RAS registers. If CFGRAMPROTEN is set to HIGH, it implies that errors are detected and, if possible, corrected, but are not recorded to RAS registers.

You can use the CFGITCMEN<m> signal to enable the *Instruction Tightly Coupled Memory* (ITCM) when leaving reset.

To initialize the TCM RAM without causing any spurious errors to be reported, follow these rules:

- If the *ACE-Lite Subordinate* (ACELS) interface is used to initialize a TCM with ECC enabled, AXI-Lite subordinate transactions must start at 128-bit aligned addresses, writing continuous blocks of memory of at least 64 bytes each and all bytes in the block enabled.
- If initialization is done by running code on the Cortex®-R82AE processor, this is best done by a loop of stores that write to the whole of the TCM memory. For both TCMs use *Store Pair* (STP) instruction to 128-bit aligned addresses.
- If you are initializing the ITCM with your program code, ensure that:
  - At least 128 bytes past the end of your program are also initialized to a known value.
  - Any remaining uninitialized parts of the ITCM should be marked as Execute-never, by programming the appropriate *Memory Protection Unit* (MPU) regions or appropriate *Memory Management Unit* (MMU) pages.

### 7.2.3 Using TCMs from reset

You can use the CFGITCMENm signal to enable the *Instruction Tightly Coupled Memory* (ITCM) from reset, the CFGITCMBASEADDRm signal to select the ITCM base address, and the CFGRVBARADDRm to select the reset vector address to fall within the ITCM address range. This enables you to configure the processor to boot from *Tightly Coupled Memories* (TCMs) but, to do this, the TCMs must first be preloaded with the boot code.

The Cortex®-R82AE processor has CPUHALTm input for each core that, when asserted, prevents the core from starting to execute instructions out of reset. This enables the TCMs to be preloaded before the core boots. If an external debug request is made before this input is deasserted, then the core waits until CPUHALTm has been deasserted, and then enters debug halt state before executing any instructions.



Note

ECC error reporting in the TCMs is suppressed when the processor core is in HALT (CPUHALTm = 1), except where an explicit read request targeting the TCMs has been received on the *ACE-Lite Subordinate* (ACELS) port.



The CPUHALTm input can be asserted while the processor is in reset to prevent the processor from fetching and executing instructions after coming out of reset. While the processor is halted in this way, the TCMs can be preloaded with the appropriate data. When the CPUHALTm input is deasserted, the processor starts fetching instructions from the reset vector address in the normal way.

**Note**

When CPUHALTm has been deasserted to start the processor fetching, it must not be asserted again except when the core is under core warm or powerup reset.

## 7.3 Initializing LLRAM

The Cortex®-R82AE processor has an optional *Low-latency RAM* (LLRAM) manager interface that is shared among the cores within the cluster.

You can configure the Cortex®-R82AE processor to:

- Enable the LLRAM out of reset.
- Boot out of an initialized LLRAM.

The LLRAM can be initialized by any core in the cluster directly or by an external agent. If an external agent is used, the Cortex®-R82AE processor supports enabling initialization of LLRAM before a core in the cluster completes its reset exception sequence and setting the reset vector address to point into the initialized LLRAM.

**Note**

Before initializing the LLRAM:

- If using a DMA, ensure that the PDCLUSTER power domain is ON or PPU\_RST\_STATE is set to 1.
- If using memory copy or debugger, ensure that both PDCLUSTER and PDCPU<m> power domains are ON or PPU\_RST\_STATE is set to 1.

### 7.3.1 Preloading LLRAM

You can write data to the memory that is connected to the *Low-latency RAM* (LLRAM) port by using either store instructions or the *ACE-Lite Subordinate* (ACELS) interface.

Depending on the method you choose, you might require:

- Particular hardware on the SoC that you are using, such as a DMA engine.
- Boot code.
- A debugger connected to the processor.

The methods to preload the memory that is connected to the LLRAM port include:

#### Memory copy with running boot code

The boot code includes a memory copy routine that reads data from an external memory, and writes it into the memory that is connected to the LLRAM port. You must enable the LLRAM to do this.

#### Copy data from the Debug Communications Channel

The boot code includes a routine to read data from the *Debug Communications Channel* (DCC) and write it into the memory that is connected to the LLRAM port. The debug host feeds the data for this operation into the DCC by writing to the appropriate registers on the processor APB debug interface.

#### Execute code in debug halt state

The debug host puts the Cortex®-R82AE processor into debug halt state and then feeds instructions into it through the *External Debug Instruction Transfer Register* (EDITR). The Cortex®-R82AE processor executes these instructions, as an alternative to using boot code in either of the two methods previously described.

#### DMA into LLRAM

The SoC includes a DMA device that reads data from a ROM and writes it to the memory that is connected to the LLRAM port through the ACELS interface.

### 7.3.2 Using LLRAM from reset

You can use the CFGLLRAMEN signal to enable the *Low-latency LLRAM* (LLRAM) from reset, the CFGLLRAMBASEADDR signal to select the LLRAM base address, and the CFGRVBARADDRm to select the reset vector address to fall within the LLRAM address range. This enables you to configure the processor to boot from LLRAM but, to do this, the memory that is connected to the LLRAM port must first be preloaded with the boot code.

The Cortex®-R82AE processor has CPUHALTm input for each core that, when asserted, prevents the core from starting to execute instructions out of reset. This enables the LLRAM to be preloaded before the core boots. If an external debug request is made before this input is deasserted, then the core waits until CPUHALTm has been deasserted, and then enters debug halt state before executing any instructions.

If the PDCPU<m> power domain is ON, the CPUHALTm input can be asserted while the processor is in reset to prevent the processor from fetching and executing instructions after coming out of reset. While the processor is halted in this way, the memory that is connected to the LLRAM can be preloaded with the appropriate data.

When the CPUHALTm input is deasserted, the processor starts fetching instructions from the reset vector address in the normal way.

**Note**

When CPUHALTm has been deasserted to start the processor fetching, it must not be asserted again except when the core is under core warm or powerup reset.

## 7.4 Disabling EL2

The Cortex®-R82AE processor always boots into EL2.

If you do not need to use EL2 after the bootup process is complete, you can program the Cortex®-R82AE processor and switch to EL1 so that it can never return to EL2 until the next reset. This involves setting all exceptions to be taken at EL1 and disabling `hvc` and the EL2-controlled *Memory Protection Unit* (MPU).

To disable EL2 and enter EL1:

- Program the `ACTLR_EL2` register because it defaults to only allowing EL2 accesses. `ACTLR_EL2` controls whether EL1 can access various processor resources. Other registers default to allowing accesses at EL1 from reset.
- Program the `CPTR_EL2` register because it resets to **UNKNOWN** values. `CPTR_EL2` controls whether various EL1 architectural features are trapped.
- Program the following EL2 generic timer registers to appropriate values because their fields reset to **UNKNOWN** values.
  - `CNTHCTL_EL2` fields can control whether various EL0 and EL1 timer register accesses are trapped to EL2.
  - `CNTHPS_CTL_EL2` fields control timer interrupts for the EL2 physical timer.
- Program the `VTCR_EL2` register because it resets to **UNKNOWN** values. `VTCR_EL2` controls the memory system translations.
- Program the rest of the `HCR_EL2` register fields because they reset to **UNKNOWN** values. For example, disable all traps to EL2, disable stage 2 address translation, disable default cacheability, route interrupts to EL1, disable virtual interrupts.
- Set `VBAR_EL1` to the correct location for the vector table.
- Disable the `hvc` instruction by setting `HCR_EL2.HCD` to 1.
- Set `ELR_EL2` and `SPSR_EL2` to point to the entry point and the desired state of the EL1 code and call `ERET`.

## 8. Memory system

This chapter describes the various memories and memory interfaces of the Cortex®-R82AE processor.

### 8.1 About the memory system

The Cortex®-R82AE processor memory system provides various memories and interfaces each tailored to different requirements.

The memory system includes memories and interfaces either private to each core or shared among the cores. Some memories and interfaces are optional so that you can configure the memory system according to your system requirements.



Note

- When you choose to exclude the optional ITCM and DTCM, the logic is removed.
- When you choose to exclude the optional L2 memory, the logic is always present but the RAM size is 0.
- When you choose to exclude the optional LLRAM, SPP, and LLPP interfaces, all the associated logic is removed. See [1.3.1 Configuration parameters](#) on page 27 for more information.

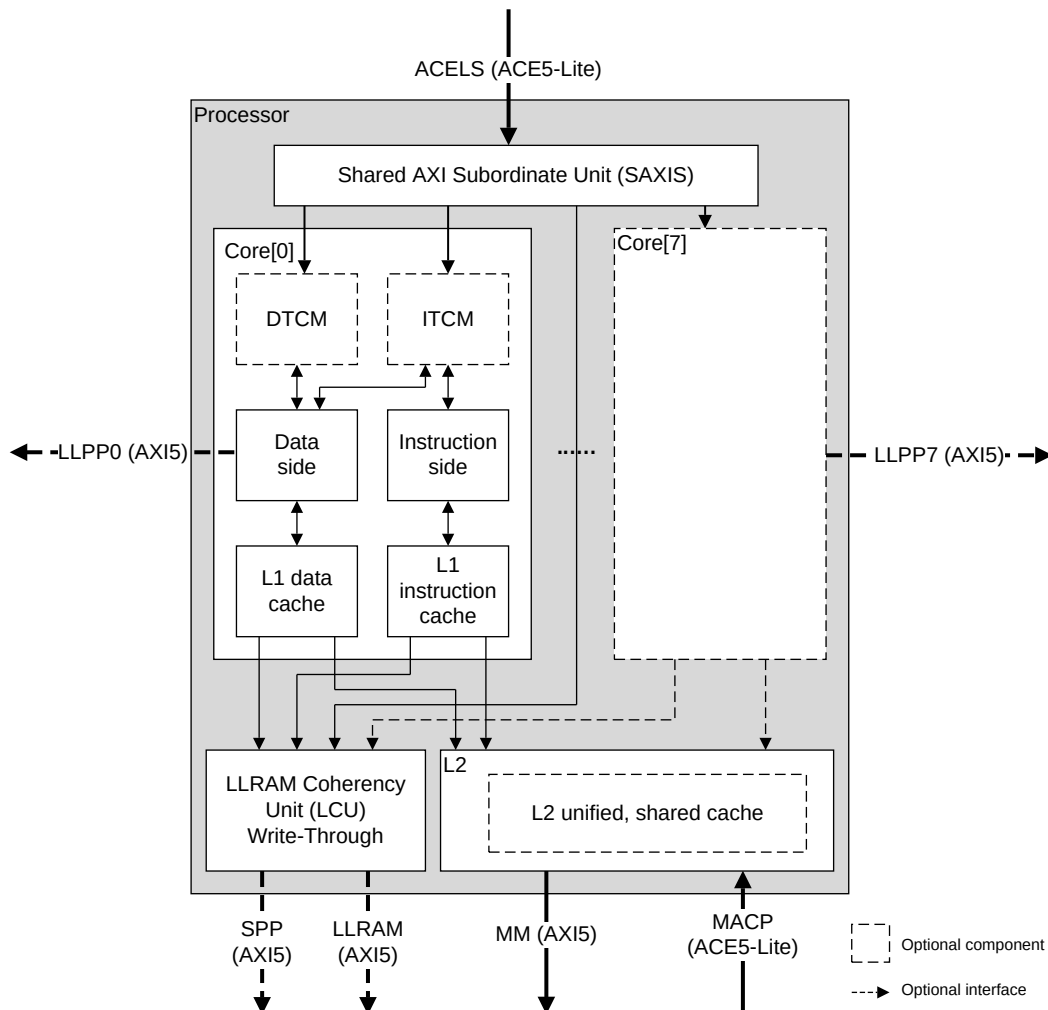
The memory system consists of:

- Memories private to each core:
  - An L1 instruction cache.
  - An L1 data cache.
  - An optional *Instruction Tightly Coupled Memory* (ITCM) for instructions and data.
  - An optional *Data Tightly Coupled Memory* (DTCM) for data.
- An optional, per-core AXI5 32-bit *Low-latency Peripheral Port* (LLPP) manager interface.
- Configurable 40 or 48-bit physical address width.
- An optional, shared, and unified L2 cache.
- A shared *Main Manager* (MM) interface implemented as either CHI.E or AXI5 256-bit port.
- An optional and shared AXI5 64-bit *Shared Peripheral Port* (SPP) manager interface.
- An optional and shared AXI5 256-bit *Low-latency RAM* (LLRAM) manager interface.
- A shared ACE5-Lite 128-bit *Main Accelerator Coherency Port* (MACP) subordinate interface for external access to MM address ranges.
- A shared 128-bit *ACE-Lite Subordinate* (ACELS) interface used for two purposes:

- As an LLRAM Accelerator Coherency Port (ACP) that enables coherent external access to the LLRAM.
- As a TCM subordinate that enables external access such as *Direct Memory Access* (DMA) to the TCMs within the cores.

The following figure shows the Cortex®-R82AE processor memory system and external interfaces.

**Figure 8-1: Memory system**



The TCM, LLPP, SPP, and LLRAM base addresses are configurable through top-level \*BASEADDR pins. See [1.3.2 Integration-time configuration options](#) on page 33 for more information on these pins. Software has read-only access to those base addresses through related region registers. See [A.2.2.39 IMP\\_ITCMREGIONR\\_EL1, ITCM Region Register](#) on page 529, [A.2.2.40 IMP\\_DTCMREGIONR\\_EL1, DTCM Region Register](#) on page 532, [A.2.2.41 IMP\\_LLPPREGIONR\\_EL1, LLPP Region Register](#) on page 535, [A.2.2.43 IMP\\_SPPREGIONR\\_EL1,](#)

[SPP Region Register](#) on page 540, and [A.2.2.42 IMP\\_LLDRAMREGIONR\\_EL1, LLDRAM Region Register](#) on page 538 for more information on these registers.

The Cortex®-R82AE processor provides protection against 1-bit and 2-bit errors for all functional RAMs. Where an error can cause a functional impact Cortex®-R82AE implements a *Single Error Correct Double Error Detect* (SECCDED) scheme if correction is required or a *Double Error Detect* (DED) scheme otherwise.

**Note**

DED ECC is provided for TCMs, the L1 data cache data RAMs, L1 data cache dirty RAMs, L2 cache tag and data RAMs, L2 cache data buffers, and L2 and LCU duplicates of L1 tag RAMs. DED ECC is provided for the L1 instruction cache data RAMs, L1 data cache tag RAMs, L1 instruction cache tag RAMs, L2 TLB data RAMs, and L2 TLB tag RAMs. L2 cache replacement RAM and branch predictor RAMs are not protected.

The Cortex®-R82AE processor provides optional bus interface protection to protect the link between the ports on the processor and the interconnect. The bus interface protection follows the AMBA® standard wherever AMBA protocols are used and, as a result, provides interoperability with any interconnect supporting the AMBA® standard. Where AMBA protocols are not used an odd-parity scheme is used, with one parity bit protecting up to 8 bits.

**Note**

Systems with safety requirements typically require diagnostics for memory accesses made by the processor. This is to protect against faults which may occur in the wiring or in the interconnect logic between the processor and the ultimate subordinate. If your system requires diagnostics for transactions between the Cortex®-R82AE processor and the other requesters and subordinates, then you should include an interconnect with appropriate safety mechanisms for detecting faults within your system.

The Cortex®-R82AE processor provides optional bus interface protection according to the AMBA® standard Data Check protocols on all signals for the following interfaces:

- MM
- LLDRAM
- SPP
- MACP
- ACELS
- LLPP
- GIC AXI4-Stream interface
- The Debug AXI4 interfaces with the debug block have protection for the default access and response which is generated if the debug block is powered down, as well as inadvertent activation protection.
- Utility bus AXI5 interface

The Cortex®-R82AE processor memory system provides various memories and interfaces each tailored to different requirements. The aim is that some memories and interfaces are used for more critical real-time requirements and some for less critical real-time requirements. The more real-time critical context is also able to access the less real-time critical interfaces and memories although such an access might not be desirable depending on the system design.

The Cortex®-R82AE processor memories and interfaces can be ordered as follows in terms of meeting critical real-time requirements:

1. TCMs are the most deterministic.
2. LLRAM, cached through the L1 caches, is more deterministic than the MM but less deterministic than the TCMs.
3. MM, cached through the L1 and L2 caches, is the least deterministic.

LLPP is a similar level of determinism to TCMs, and SPP is a similar level of determinism to LLRAM.

The TCMs provide the most deterministic timing for memory accesses. The ITCM enables low-latency access for instructions and data. The DTCM provides low-latency access for data only. The ITCM and the DTCM are private to each core and their contents are not cached.

The TCM interface includes a full crossbar switch that allows concurrent access from three requesters (instruction side, data side, and ACELS) to the ITCM and concurrent access from two requesters (data side and ACELS) to the DTCM. If one or more requesters attempt to access the same TCM, the TCM interface arbitrates between the requests on a fixed priority scheme with Quality of Service (QoS) mechanisms. See [8.15.4 Quality of Service](#) on page 215 for information on QoS.

The TCMs support memory testing via *Memory Built-In Self Test* (MBIST).

Where access timing determinism is less critical but fast access is still required, L1 instruction cache and L1 data cache can be used. L1 instruction cache and L1 data cache are used to cache instructions and data respectively from the MM port and the LLRAM port. The cache behavior depends on the memory attributes. The L1 memories support cache maintenance operations according to the Arm® architecture and memory testing via MBIST.

The LLRAM interface is optimized for deterministic, low-latency access. Accesses from the LLRAM interface can be cached in the L1 cache if the memory attributes are cacheable. These accesses are only cached Write-Through to improve the LLRAM determinism by avoiding waiting for evictions. The LLRAM port is expected to be connected directly to an SRAM controller for optimal performance. Under this assumption, the LLRAM is expected to have better real-time characteristics compared to the MM port. A real-time context is also able to access the MM port, although such an access might not be desirable depending on the system design.

The L2 cache is unified and therefore it can cache both instructions and data. L2 can cache instructions and data only from the MM port but not the LLRAM port. Accesses from the MM port are only cached Write-Back in the L1 and L2 caches to limit the bandwidth to the main memory.

The following table shows which accesses are allowed in the *Protected Memory System Architecture* (PMSA) and *Virtual Memory System Architecture* (VMSA) contexts.

**Table 8-1: Accesses in PMSA and VMSA**

Memory system	PMSA	VMSA
ITCM and DTCM	Allowed	Not allowed (aborted)
LLRAM	Allowed	Page table walk accesses are not allowed. Generates synchronous External abort on translation table walk or hardware update of translation table. The level depends on the current level of the pagewalk.  General accesses are allowed.
MM	Allowed	Allowed
LLPP	Allowed	Allowed
SPP	Allowed	Allowed

## 8.2 TCM memories

The *Tightly Coupled Memories* (TCMs) have the most deterministic memory access timing. They are expected to store the most critical real-time code and data, such as interrupt handlers and memory stacks.

Each core within the Cortex®-R82AE processor has two optional TCMs, *Instruction Tightly Coupled Memory* (ITCM) and *Data Tightly Coupled Memory* (DTCM), implemented as RAMs. Optional here means that the minimum required logic is always present but the size can be 0KB.

ITCMs are unified and can be used for both instructions and data. They are typically used for instruction side accesses such as storing critical code and exception handlers, but also available for data side read and write accesses such as accessing literal pools or initializing program code. DTCMs are dedicated for data side accesses only, such as stack operations and inter-thread data sharing.



Note

Both ITCM and DTCM are optimized to allow concurrent accesses from multiple sources. Each TCM is organized in two logical banks. Core instruction-side read accesses (for the ITCM only), core data-side read/write accesses, and external read/write accesses from *ACE-Lite Subordinate* (ACELS) interface can simultaneously access a TCM in the same cycle if the accesses are on different TCM banks. Simultaneous requests to the same bank are arbitrated in a fair way to minimize the core stalls.

You can implement each TCM independently to sizes of 0KB, 16KB, 32KB, 64KB, 128KB, 256KB, 512KB, or 1MB. A size of 0KB indicates that the TCM is not implemented.

All writes to the ITCM that are less than 64 bits wide will always require a read-modify-write procedure. Use 64 bit wide accesses to optimize ITCM writes.



The base address and the size of each TCM and whether it is enabled is visible in the respective TCM region register ([A.2.2.39 IMP\\_ITCMREGIONR\\_EL1, ITCM Region Register](#) on page 529 and [A.2.2.40 IMP\\_DTCMREGIONR\\_EL1, DTCM Region Register](#) on page 532).

If the CFGITCMENm input for core m is asserted at reset, the ITCM in that core is enabled. The ITCM base address is set by the CFGITCMBASEADDRm configuration inputs of core m.

The DTCM remains disabled unless a write to IMP\_DTCMREGIONR\_EL1 enables it. The DTCM base address is set by the CFGDTCMBASEADDRm configuration inputs of core m.

If the TCMs are implemented and not enabled, accesses to the TCM regions generate aborts.

Both TCMs are accessible by the software running at EL1 or EL0 only if it operates in a *Protected Memory System Architecture* (PMSA) context.



TCM accesses are not supported in *Virtual Memory System Architecture* (VMSA) context.

---

Software running at EL2 can always access the TCMs. Writes to TCM region registers from EL1 can be trapped to the hypervisor, running at EL2, by setting the register bit HCR\_EL2.TIDCP=1 or ACTLR\_EL2.REGIONS=0.

The TCMs can be accessed for reads and writes by external agents through the *ACE-Lite Subordinate* (ACELS) port, implemented as a ACE5-Lite 128-bit shared subordinate interface.

You can implement each TCM independently with a wait state of 0 to 3 cycles on access, meaning that accesses to that TCM incur that many cycles of latency. If you implement some, but not all TCMs with wait cycles, the performance of the TCMs might differ from each other.

ITCMs provide up to 128-bit per cycle of bandwidth to the instruction side, up to 128-bit per cycle of bandwidth to the data side and up to 128-bit per cycle of bandwidth to the external agent through the ACELS. They allow for 256-bit per cycle of total bandwidth when two of these sources concurrently access oppositely 128-bit-aligned locations.

DTCMs provide up to 128-bit per cycle of bandwidth to the data side and up to 128-bit per cycle of bandwidth to the external agent through the ACELS. This allows 256-bit per cycle of total bandwidth when the core and an external agent through the ACELS concurrently access oppositely 128-bit-aligned data locations. Instruction side accesses to DTCMs are not allowed.

Load and store exclusive accesses performed to the TCMs are handled by the local exclusive monitor.

TCMs are private to each core without any internal mechanism for one core to access another core's TCMs. An exception to this rule is for Split-Lock configurations, where the primary core can access the shadow core's TCMs. In a Split-Lock configuration, all of the TCM RAMs are used by a core in Split-mode. When in locked-mode, the number of cores is halved, so half of the TCM (and

L1 cache) RAMs are not associated with a logical core. The Cortex®-R82AE processor still enables accessing these TCM RAMs for reads and writes through the ACELS port when in lock-step. These accesses incur additional 4 cycles of latency.

The Cortex®-R82AE processor supports SECDED ECC protection with 64-bit chunk for the ITCM and optional SECDED ECC protection with 32-bit chunk for the DTCM.

For more information on TCM memory protection behavior, see [10.2 Memory protection behavior](#) on page 241.

### TCM attributes and permissions

Enabled TCMs always behave as Non-cacheable Non-shareable Normal memory. This is irrespective of the memory type attributes defined in the *Memory Protection Unit* (MPU) for a memory region containing addresses that are held in the TCM. Access permissions for TCM accesses are the same as the permission attributes that the MPU assigns to the same address.

## 8.3 L1 memory system

Each core within the Cortex®-R82AE processor has separate L1 instruction and L1 data caches. You can configure the L1 instruction and data caches within a core independently from each other and also from the L1 caches in other cores during rendering.

The L1 instruction cache size can be configured to 16KB, 32KB, 64KB, or 128KB. The L1 data cache size can be configured to 16KB, 32KB, or 64KB.

L1 caches improve the average performance of programs that do not use the *Tightly Coupled Memories* (TCMs). Because the performance of an individual transaction depends on whether the cache hits or misses, performance from L1 caches is less deterministic than the TCMs.

Both the L1 instruction and L1 data cache can cache data from the *Main Manager* (MM) port and the *Low-latency RAM* (LLRAM) port. The L1 data cache supports Write-Back caching for MM locations and Write-Through caching for LLRAM locations.

The L1 caches fetch critical-word first. Linefills support write streaming and are non-blocking to subsequent cache accesses. The *Memory Protection Unit* (MPU) and the *Memory Management Unit* (MMU) control the cacheability of accesses. The MPU and MMU also provide allocation hints, although these may be automatically overridden to improve the performance when write streaming is detected. For more information on write streaming see, [8.3.2.4 Write Streaming Mode](#) on page 132.

The Cortex®-R82AE processor includes both instruction side and data side prefetchers to improve the cache hit rate, and therefore, the performance. The prefetchers can anticipate several variants of cache access patterns, and request linefills to the L1 caches and also to the shared L2 cache.

The Cortex®-R82AE processor does not include any virtually indexed caches that could generate aliasing issues, so cache maintenance is not required on context switches.

The L1 caches are automatically invalidated after a core reset, unless the reset is because of an MBIST request or for debug recovery.

The Cortex®-R82AE processor provides an *Error Correcting Code* (ECC) scheme for detecting and correcting errors. L1 instruction cache RAMs and L1 data cache tag RAMs are protected with *Double Error Detect* (DED) scheme. L1 data cache data RAMs are protected with *Single Error Correct Double Error Detect* (SECEDED) scheme. ECC codes are generated and checked automatically when ECC is enabled. Errors are corrected when possible, either by invalidating a copy of the line and refetching it, or via ECC correction logic (with SECEDED protection only). Otherwise an abort is taken by the Cortex®-R82AE processor if the error is about to be consumed or a poison code is written to the cache. The caches are tolerant to a limited number of hard errors.



In Cortex®-R82AE RAM protection is always present.

---

For more information on L1 memory protection behavior, see [10.2 Memory protection behavior](#) on page 241.

### L1 instruction side memory system

The L1 instruction side memory system provides an instruction stream to the *Data Processing Unit* (DPU). Its key features are:

- 64-byte instruction side cache line length.
- 4-way set associative L1 instruction cache.
- 128-bit read interface to the shared L2 memory system.
- Instruction side prefetcher that prefetches cache lines ahead of the current point of execution from the MM or LLRAM interfaces and allocates them into the L1 instruction cache.

The Cortex®-R82AE processor uses extensive branch prediction to improve *Instructions Per Cycle* (IPC) and power efficiency.

### L1 data side memory system

The L1 data side memory system responds to load and store requests from the DPU. It also responds to L2 coherency logic snoop requests from other cores or external agents. Its key features are:

- 64-byte data side cache line length.
- 4-way set associative L1 data cache.
- Read buffer that services both the *Data Cache Unit* (DCU), and the *Instruction Fetch Unit* (IFU).
- 128-bit read path from the data L1 memory system to the datapath.
- 128-bit write path from the datapath to the L1 memory system.
- Merging store buffer capability which writes to all types of memory (Device, Normal Cacheable and Normal Non-cacheable).

- Data side prefetcher that prefetches data cache lines ahead of the current point of execution from the MM or LLRAM interfaces and allocates them into the L1 data cache. Data side prefetcher is capable of detecting both constant and patterns of strides.

The L1 data side memory system includes forwarding paths to reduce load-to-use time where possible. These are only supported when data accesses are made in little-endian format.

### 8.3.1 L1 instruction memory system

The L1 instruction cache is organised as a *Virtually Indexed Physically Tagged* (VIPT) cache.

The L1 instruction side memory system provides an instruction stream to the *Data Processing Unit* (DPU).

#### 8.3.1.1 Instruction cache disabled behavior

If the SCTLR\_EL1.I bit is set to 0, load and store instructions at EL1 and EL0 do not access any of the L1 instruction or L2 caches. If the SCTLR\_EL2.I bit is set to 0, load and store instructions at EL2 do not access any of the L1 instruction or L2 caches.

The SCTLR\_EL1.I and SCTLR\_EL2.I bits control whether accesses from the core can look up and allocate into the L1 instruction cache and unified L2 cache. L1 instruction cache maintenance operations execute normally, regardless of how the SCTLR\_EL1.I and SCTLR\_EL2.I bits are set.

If the instruction cache is disabled, all instruction fetches to cacheable memory are treated as if they were non-cacheable. This means that instruction fetches might not be coherent with caches in other cores and software must take account of this.

The Cortex®-R82AE processor does not allocate lines into the instruction cache when the instruction cache is disabled or the memory is marked as non-cacheable.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

#### 8.3.1.2 Instruction cache speculative memory accesses

Instructions that are fetched may get discarded and in that sense are speculative, as there can be several unresolved branches in the pipeline.

A branch instruction or exception in the code stream can cause a pipeline flush, discarding the currently fetched instructions. Instruction fetches to Device type memory take a synchronous prefetch abort.

Device memory areas must be marked with the translation table descriptor attribute bit *Execute-never* (XN). The device and code address spaces must be separated in the physical memory map. This separation prevents speculative fetches to read-sensitive devices.

If the instruction cache is enabled and if the instruction fetches miss in the L1 instruction cache, instruction fetches can still look up and return data from the L2 cache or L1 data cache if appropriate, or from the external interfaces otherwise. Instruction fetches never result in a line being allocated in the L1 data cache but may result in the line being allocated into the L2 cache if the L2 cache is enabled.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

### 8.3.1.3 Instruction cache invalidate on reset

The Arm®v8-R AArch64 architecture supports the system instructions `IC IALLU` and `IC IALLUIS` to invalidate the entire instruction cache.

The Cortex®-R82AE processor automatically invalidates instruction caches on reset unless suppressed with the debug recovery P-Channel state or an MBIST request. It is therefore not necessary for software to invalidate the instruction caches on startup.

### 8.3.1.4 Branch prediction

The Cortex®-R82AE processor contains branch prediction hardware, also known as program flow prediction.

Branch prediction increases overall performance and reduces power consumption. With branch prediction disabled, all taken branches incur a penalty that is associated with flushing the pipeline.

To avoid this penalty, the branch prediction hardware predicts:

- If a conditional or unconditional branch is to be taken.
- The address to which the branch goes, known as the branch target address.

For conditional branches, the hardware predicts if the branch is to be taken and also the branch target address. For unconditional branches, only the branch target address is predicted.

The hardware contains the following functionality:

- A *Branch Target Address Cache* (BTAC) holding the branch target address of previously taken indirect branches.
- A dynamic branch predictor.
- The return stack, a stack of nested subroutine return addresses.
- A static branch predictor.

### Predicted and non-predicted instructions

As a rule, the flow prediction hardware predicts all branch instructions regardless of the addressing mode, and includes:

- Conditional branches.

- Unconditional branches.
- Indirect branches that are associated with procedure call and return instructions.

Exception return and exception generating instructions are not predicted.

### Return stack

On execution of Branch with Link instructions, the return stack stores the address that is equal to the link register value stored in X30.

The following instructions cause a return stack push:

- BL
- BLR
- BLRAA, BLRAAZ, BLRAB, BLRABZ

The return instructions cause a return stack pop. These include:

- RET
- RETAA, RETAB

The exception return instructions (`ERET`, `ERETA`, and `ERETAB`) and exception generating instructions (`SVC`, `HVC`, `BRK`, and `HLT`) are not predicted because they can change the privilege mode. Prefetching stops when any of these instructions are encountered until they are committed. Then the fetch resumes from the appropriate point in the program flow.

Similarly, certain barrier instructions such as `SB` and `ISB` also cause prefetching to stop, to help lower the attack surface of various side-channel attacks.

#### 8.3.1.5 Instruction prefetching

The Cortex®-R82AE processor includes an instruction side prefetcher that prefetches cache lines ahead of the current point of execution from the *Main Manager* (MM) or *Low-latency RAM* (LLRAM) interfaces and allocates them into the L1 instruction cache.

The Cortex®-R82AE processor has `IMP_CPUACTLR_EL1` system register controls for the instruction side prefetcher to:

- Enable or disable the prefetcher with or without power-aware throttling mechanisms.
- Configure how far ahead from the current point of execution to prefetch, that is, 1 to 4 cache lines ahead of the current line.
- Configure whether the prefetcher always prefetches ahead or only starts prefetching ahead on an L1 instruction cache miss.

## 8.3.2 L1 data memory system

The L1 data cache is organized as a *Physically Indexed Physically Tagged* (PIPT) cache.

### 8.3.2.1 Data cache disabled behavior

If the SCTLR\_EL1.C bit is set to 0, load and store instructions at EL1 and EL0 do not access any of the L1 data or L2 caches. If the SCTLR\_EL2.C bit is set to 0, load and store instructions at EL2 do not access any of the L1 data or L2 caches.

The SCTLR\_EL1.C and SCTLR\_EL2.C bits control whether accesses from the core can look up and allocate into the L1 data cache and unified L2 cache. L1 data cache maintenance operations execute normally, regardless of how the SCTLR\_EL1.C and SCTLR\_EL2.C bits are set.

If the L1 data and L2 caches are disabled at the current Exception level, then the following applies:

- All load and store instructions to cacheable memory are treated as if they were non-cacheable. Therefore, they are not coherent with the caches in this core or the caches in other cores, and software must take this into account.

The L1 data and L2 caches cannot be disabled independently.

### 8.3.2.2 Data cache maintenance considerations

The `DC INVAC` instruction performs an invalidate of the target address.

If the data is dirty, a clean is performed before the invalidate.

The `DC ISW`, `DC CSW`, and `DC CISW` instructions perform both a clean and invalidate of the target set/way. The value of HCR\_EL2.SWIO has no effect and it is implemented as `RES1` in the Cortex®-R82AE processor.



**Note**

There might be implications to real-time characteristics of *Low-latency RAM* (LLRAM) accesses when `DC ISW`, `DC CSW`, or `DC CISW` instructions are executed. See [8.15 Real-time considerations](#) on page 203 for more information.

### 8.3.2.3 Data cache coherency

The Cortex®-R82AE processor uses the MESI protocol to maintain data coherency between multiple cores.

MESI describes the state that a shareable line in a L1 data cache can be in:

<b>M</b>	Modified/ <i>UniqueDirty</i> (UD). The line is in only this cache and is dirty.
<b>E</b>	Exclusive/ <i>UniqueClean</i> (UC). The line is in only this cache and is clean.

- S** Shared/*SharedClean* (SC). The line is possibly in more than one cache and is clean.
- I** Invalid/*Invalid* (I). The line is not in this cache.

The *Data Cache Unit* (DCU), the L2, and the *LLRAM Coherency Unit* (LCU) store the MESI state of the cache lines in the tag, dirty, and the L1 duplicate tag RAMs.



**Note**

The names UniqueDirty, SharedDirty, UniqueClean, SharedClean, and Invalid are the AMBA names for the cache states. The Cortex®-R82AE processor does not use the SharedDirty AMBA state.

### 8.3.2.4 Write Streaming Mode

A cache line is allocated to the L1 cache on either a read miss or a write miss.

However, there are some situations where allocating on writes is not desirable. For example, when executing the C standard library `memset()` function to clear a large block of memory to a known value. Writes of large blocks of data can pollute the cache with unnecessary data. It can also waste power and performance if a linefill must be performed only to discard the linefill data because the entire line was subsequently written by the `memset()`.

To counter this, the *Store Unit* (STU) includes logic to detect when the core has written at least a byte in all the four chunks of the cacheline, before the linefill completes. The granularity of a chunk is 128 bits. The granularity of a cacheline is 512 bits.

If this situation is detected on a configurable number of consecutive linefills, then it switches into write streaming mode. This is sometimes referred to as read allocate mode.

When in write streaming mode:

- Loads behave as normal and can still cause linefills.
- Writes still lookup in the cache but if they miss then, they write out to L2 cache rather than starting a linefill.



**Note**

More than the specified number of linefills might be observed on the AXI or CHI manager interface, before the STU detects that the programmed number of full cache lines have been written and switches to write streaming mode.

The STU continues in write streaming mode until it detects either a cacheable write burst that is not a full cache line, or there is a load from the same line as is currently being stored to.

In the Cortex®-R82AE processor:

- `IMP_CPUACTLR_EL1.DL1WS` configures the L1 write streaming mode threshold.
- `IMP_CPUACTLR_EL1.DL2WS` configures the L2 write streaming mode threshold.



### 8.3.2.5 Data cache invalidate on reset

The Arm®v8-R AArch64 architecture does not support an operation to invalidate the entire data cache.

The Cortex®-R82AE processor automatically invalidates data caches on reset unless suppressed with the debug recovery P-Channel state or an MBIST request. It is therefore not necessary for software to invalidate the data caches on startup.

If software requires this function later after the startup, it must be constructed by iterating over the cache geometry and executing a series of individual invalidate by set/way instructions.

### 8.3.2.6 Instructions implemented by the L1 memory system

This section describes the instructions implemented by the L1 memory system.

#### Atomic instructions

The Cortex®-R82AE processor supports the atomic instructions added in the Arm®v8.1 architecture.

Accesses targeting the *Main Manager* (MM) interface perform all the atomics either in the L1 data cache or in the interconnect outside the Cortex®-R82AE processor. MM atomic instructions to cacheable memory can be performed as either near atomics or far atomics, depending on where the cache line containing the data resides:

- Cacheable MM atomics are executed near if BROADCASTATOMICM is LOW.
- Non-cacheable/Device LLRAM atomics are executed far when CFGLLRAMSHARED is HIGH and BROADCASTATOMICL is high. When CFGLLRAMSHARED is HIGH and BROADCASTATOMICL is LOW, they are aborted by the Cortex®-R82AE processor. When CFGLLRAMSHARED is LOW, they are executed near.
- Cacheable MM atomics are executed near if the shareability domain does not extend to the interconnect (BROADCASTOUTERM is LOW for shareable atomics).
- Cacheable MM atomics are executed near if they hit in the cache in a unique state.
- Unaligned cacheable MM atomics are always executed near.
- Unaligned atomics on the *Tightly Coupled Memories* (TCMs) are always executed near.
- Unaligned atomics to *Low-latency RAM* (LLRAM) port, *Shared Peripheral Port* (SPP), and *Low-latency Peripheral Port* (LLPP) are not supported.
- Non-cacheable/Device MM atomics are always executed far, unless BROADCASTATOMICM is LOW in which case they are aborted by the Cortex®-R82AE processor.
- Unaligned atomics to LLRAM port are not supported.
- Atomics to SPP and LLPP are not supported.
- Cacheable MM atomics which miss in the cache are executed far if BROADCASTATOMICM is HIGH.

- Cacheable MM atomics which hit in the cache in a shared state execute far if BROADCASTATOMICM is HIGH.

The Cortex®-R82AE processor MM supports sending atomics externally to Device or Non-cacheable memory, however this depends on the interconnect also supporting atomics. If such an atomic instruction is executed when the interconnect does not support them (BROADCASTATOMICM is LOW), it results in a synchronous Data Abort for both load atomics and store atomics. If there is an external abort on an atomic, it results in a synchronous Data abort for load atomics and an asynchronous Data abort for store atomics.

The behavior of the atomic instructions can be modified by the IMP\_CPUACTLR\_EL1 register settings. For more information on the IMP\_CPUACTLR\_EL1 register, see [A.2.2.44 IMP\\_CPUACTLR\\_EL1, CPU Auxiliary Control Register](#) on page 542.

*Low-latency RAM (LLRAM)* manager interface performs all aligned atomics within the *LLRAM Coherency Unit (LCU)* at the shared level rather than in the L1 memory system or external memory. The Cortex®-R82AE processor LLRAM performs atomics to device or Non-cacheable memory within the LCU without requiring interconnect support. This is built on the assumption that the LLRAM port is connected directly to an external memory and the LLRAM manager cannot access data that is shared with other agents in the system. The Cortex®-R82AE processor can perform atomics on the LLRAM port assuming that no external agents are able to modify the memory location between the read and write operation, and caches shareable data without any support for cache coherency with external agents. This only applies when CFGLLRAMSHARED is set to 0 or when CFGLLRAMSHARED is set to 1 but for non-shareable/inner-shareable locations.

## LDAPR instructions

The Cortex®-R82AE processor supports load-acquire and store-release instructions with the RCpc consistency semantic introduced in the Armv8.4-RCpc extension, however the implementation does not make use of the ordering relaxations. Armv8.4-RCpc load-acquire and store-release instructions will still be ordered when targeting different addresses.

The instruction support is reflected in register ID\_AA64ISAR1\_EL1 where bits[23:20] are set to 0b0010 to indicate that the processor supports LDAPUR\*, STLUR\*, and LDAPR\* instructions.

For more information on the ID\_AA64ISAR1\_EL1 register, see [A.2.1.33 ID\\_AA64ISAR1\\_EL1, AArch64 Instruction Set Attribute Register 1](#) on page 384.

## Transient memory region

The Cortex®-R82AE processor has a specific behavior for memory regions that are marked as Write-Back cacheable and transient for MM and Write-Back transient or Write-Through transient for LLRAM, as defined in the Arm®v8-R AArch64 architecture.

For both MM and LLRAM, any load that is targeted at a memory region that is marked as transient, the following occurs:

- If the memory access misses in the L1 data cache, the returned cache line is allocated in the L1 data cache but is marked as transient. Where an L1 data cache allocation needs to evict an existing entry, transient locations are prioritized for eviction where possible.

For MM, any load that is targeted at a memory region that is marked as transient, the following occurs:

- On eviction, if the line is clean and marked as transient, it is not allocated into the L2 cache but is marked as invalid.

For MM, for stores that are targeted at a memory region that is marked as transient, the following occurs:

- If the store misses in the L1 data cache, the line is allocated into the L2 cache.

### Non-temporal loads

Non-temporal loads indicate to the caches that the data is likely to be used for only short periods. For example, when streaming single-use read data that is then discarded. In addition to non-temporal loads, there are also prefetch-memory (**PRFM**) hint instructions with the **STRM** qualifier.

Non-temporal loads cause allocation into the L1 data cache, with the same performance as normal loads. However, when a later linefill is allocated into the cache, the cache line marked as non-temporal has higher priority to be replaced. To prevent pollution of the L2 cache, a non-temporal line that is evicted from L1, is not allocated to L2 as would happen for a normal line.



The line is only marked as non-temporal in the cache if the core has the line in a unique state. If shared with other cores, the line is treated normally.

---

Non-temporal stores are treated the same as stores to a memory region that is marked as transient.

### 8.3.2.7 Local exclusive monitor

The Cortex®-R82AE processor L1 memory system has an architecturally defined local exclusive monitor.

This monitor is a 2-state, open and exclusive, state machine that manages Load-Exclusive or Store-Exclusive accesses and Clear-Exclusive (**CLREX**) instructions. You can use these instructions to construct semaphores, ensuring synchronization between different processes running on the core, and also between different cores that are using the same coherent memory locations for the semaphore. A Load-Exclusive instruction tags a small block of memory for exclusive access. **CTR\_EL0.ERG** defines the size of the tagged block as 16 words, one cache line.



A load/store exclusive instruction is any instruction that has a mnemonic starting with **LDX**, **LDAX**, **STX**, or **STLX**.

---

If a Load-Exclusive instruction is performed to non-cacheable shareable or device memory and is to a region of memory in the SoC that does not support exclusive accesses, the external exclusive-fail response causes a Data Abort exception with a Data Fault Status Code of 0b110101.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information about these instructions.

#### 8.3.2.7.1 Treatment of intervening STR operations

Where there is an intervening store operation between an exclusive load and an exclusive store from the same core, the intermediate store does not produce any direct effect on the local exclusive monitor.

After the exclusive load, the local monitor is in the Exclusive Access state. It remains in the Exclusive Access state after the store, and then returns to the Open Access state only after an exclusive store, a `CLREX` instruction, or an exception return.

However, if the exclusive code sequence accessed address is in cacheable memory, any eviction of the cache line containing that address clears the monitor. Arm recommends that no load or store instructions are placed between the exclusive load and the exclusive store, because these additional instructions can cause a cache eviction. Any data cache maintenance instruction can also clear the exclusive monitor.

#### 8.3.2.7.2 Exclusive monitor

In the exclusive state machine, the **IMPLEMENTATION DEFINED** transitions are as follows:

- If the monitor is in the exclusive state, and a store exclusive is performed to a different cacheline, then the store exclusive fails and does not update memory.
- If the monitor is in the exclusive state and a store exclusive is performed to a same cacheline but a different address, then the store exclusive passes and updates memory.
- If a normal store is performed to a different address, it does not affect the exclusive monitor.
- If a normal store is performed from a different core to the same address for Sharable Cacheable locations, it clears the exclusive monitor. If the store is from the same core then it does not clear the monitor.
- If a normal store is performed from a different core to the same address for Sharable Non-cacheable locations, then the global exclusive monitor in the SoC clears the exclusive monitor. If the store is from the same core then it does not clear the monitor.



If you are using load/store exclusive instructions to build semaphores, Arm recommends that you use a full cacheline per semaphore.

---

### 8.3.2.8 Data prefetching

The following section describes the software and hardware data prefetching behavior of the Cortex®-R82AE processor.

#### Hardware data prefetcher

The Cortex®-R82AE processor has a data prefetch mechanism that looks for cache line fetches with regular patterns. If the data prefetcher detects a pattern, then it signals to the memory system that memory accesses from a specified address are likely to occur soon. The memory system responds by starting new linefills to fetch the predicted addresses ahead of the instruction stream.

The Cortex®-R82AE processor can track multiple streams in parallel.

Prefetch streams end when either:

- The pattern is broken.
- A `DSB` instruction is executed.
- A `WFI` instruction or `WFE` instruction is executed.

For read streams, the prefetcher is based on the addresses. A given stream is allowed to prefetch addresses through multiple *Memory Protection Unit* (MPU) regions as long as they are cacheable and with read permissions. For more information see, [9.2.1 MPU regions](#) on page 218.

For some types of pattern, when the prefetcher is confident in the stream, it can start progressively increasing the prefetch distance ahead of the current accesses. These accesses start to allocate to the L2 cache rather than L1. Allocating to the L2 cache allows better utilization of the larger resources available at L2. Also, utilizing the L2 cache reduces the amount of pollution of the L1 cache if the stream ends or is incorrectly predicted. If the prefetching to L2 was accurate, the line will be removed from L2 and allocated to L1 when the stream reaches that address.

The `IMP_CPUACTLR_EL1` register allows you to:

- Enable or disable the prefetcher, for each target interface separately.
- Control the maximum number of prefetch streams that can be active at once.

#### Preload instructions

The Cortex®-R82AE processor supports `PLD` and `PRFM` instructions. `PLD` and `PRFM` instructions perform a lookup in the L1 cache and, in the case of a cache miss, initiate a linefill request to bring the line into the L1 cache. The `PRFM` instruction also enables targeting of a prefetch to the L2 cache. A request is sent to L2 to start a linefill, and then the instruction can retire without any data being returned to L1. `PLI`, `PLIL1KEEP` and `PLIL1STRM` are implemented as a prefetch to L2.

Use the `PLD` or `PRFM` instruction for software data prefetching where short sequences or irregular pattern fetches are required. For more information about prefetch memory and preloading caches, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

## Data Cache Zero

The Data Cache Zero by Virtual Address (DC ZVA) instruction enables a block of 64-bytes in memory, which is aligned to 64-bytes in size, to be set to 0. The DCZID\_ELO register passes this value.

The DC ZVA instruction allocates this value into the data cache using the same method as a normal store instruction.

## 8.4 L2 memory system

The Cortex®-R82AE processor has an optional unified L2 cache that is shared by all the cores in the cluster. L2 cache improves the average performance of programs that use memory within the *Main Manager* (MM) address range.

The L2 memory is unified and therefore it can cache both instructions and data. The L2 can cache instructions and data only from the MM port but not the *Low-latency RAM* (LLRAM) port. The L2 cache supports Write-Back caching for MM locations.

Because the performance of an individual transaction depends on whether the L1 and L2 caches hit or miss, performance from the L2 cache is less deterministic than the *Tightly Coupled Memories* (TCMs) or LLRAM. The L2 cache fetches critical-word first, and linefills support streaming. This prevents the blocking of subsequent cache accesses.

The *Memory Protection Unit* (MPU) and the *Memory Management Unit* (MMU) control the cacheability of accesses. They also provide allocation hints although these may be automatically overridden to improve the performance when streaming is detected.

The L2 memory subsystem consists of:

- An optional 8-way, set-associative L2 cache with a configurable size of 0KB, 96KB, 128KB, 192KB, 256KB, 384KB, 512KB, 768KB, 1MB, 1.5MB, 2MB, 3MB, or 4MB. Cache lines have a fixed length of 64 bytes.
- *Error Correcting Code* (ECC) protection for tag, data, L1 duplicate tag, and L2 data buffer RAM structures.



For information on L2 memory protection behavior, see [10.2 Memory protection behavior](#) on page 241.

---

The main features of the L2 memory system are:

- Shared and unified L2 cache.
- Organized as a *Physically Indexed Physically Tagged* (PIPT) cache.
- Duplicate PIPT L1 tag RAMs.
- Pseudo-exclusive with L1 data cache.

- Pseudo-inclusive with L1 instruction cache.
- Configurable cache slice and RAM partitions that the L2 cache implements.

The Cortex®-R82AE processor respects cacheability attributes when determining whether or not to cache data in the L2 cache.

The L2 cache supports stashing requests from the *Main Accelerator Coherency Port* (MACP) implemented as ACE-Lite and the MM if it is configured as a CHI port.

The L2 cache is invalidated automatically at reset unless the reset is because of an MBIST request or for debug recovery.

### 8.4.1 L2 cache slice integration

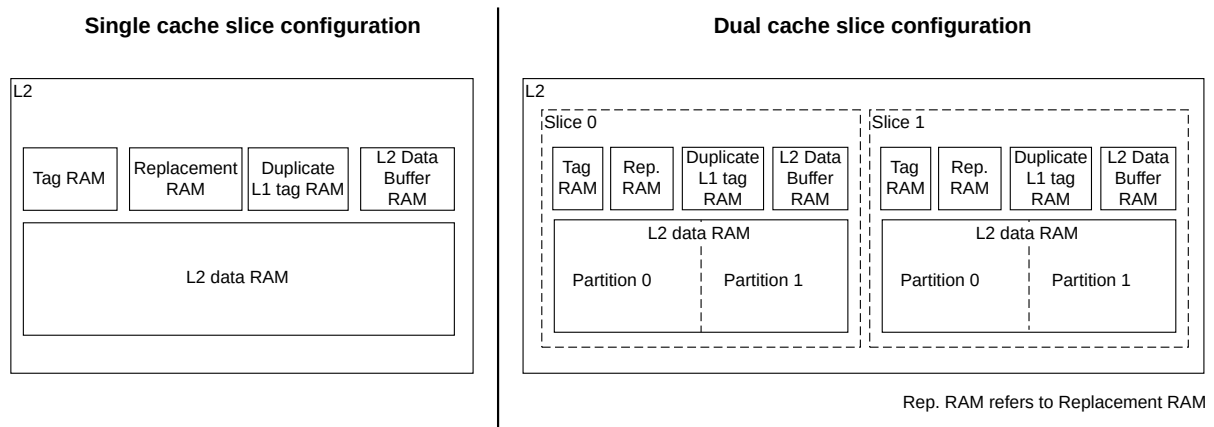
The Cortex®-R82AE processor L2 cache is implemented as either a single cache slice or a dual cache slice, depending on the configuration.

L2\_SLICES parameter controls the number of slices and RAM partitions the L2 cache implements.

A cache slice consists of data RAMs, tag RAMs, replacement RAMs, duplicate L1 tag RAMs, L2 data buffer RAMs, and associated logic.

When two cache slices are implemented, the overall cache is divided across the two slices. There is associated logic for each of the cache slices. The following figure shows the differences between a single slice configuration and a dual slice configuration.

**Figure 8-2: Comparison between a single and dual L2 cache slice configuration**



Splitting the cache into two slices improves the physical floorplan when implementing the macrocell, particularly for larger cache sizes. It also gives increased bandwidth because the two slices can be accessed in parallel.

When a dual slice configuration is implemented, the L2 cache data RAM is further divided into two partitions in order to facilitate powering down of half the data RAM when bandwidth requirements are low.

#### 8.4.1.1 Cache slice selection

For a dual cache slice implementation, requests are sent to a particular slice depending on the address and the memory attributes of the request:

- For Cacheable and Non-cacheable requests, addresses are interleaved between slice 0 and slice 1, based on address bit 6 of the request.
- Device and DVM requests are always sent to slice 0.

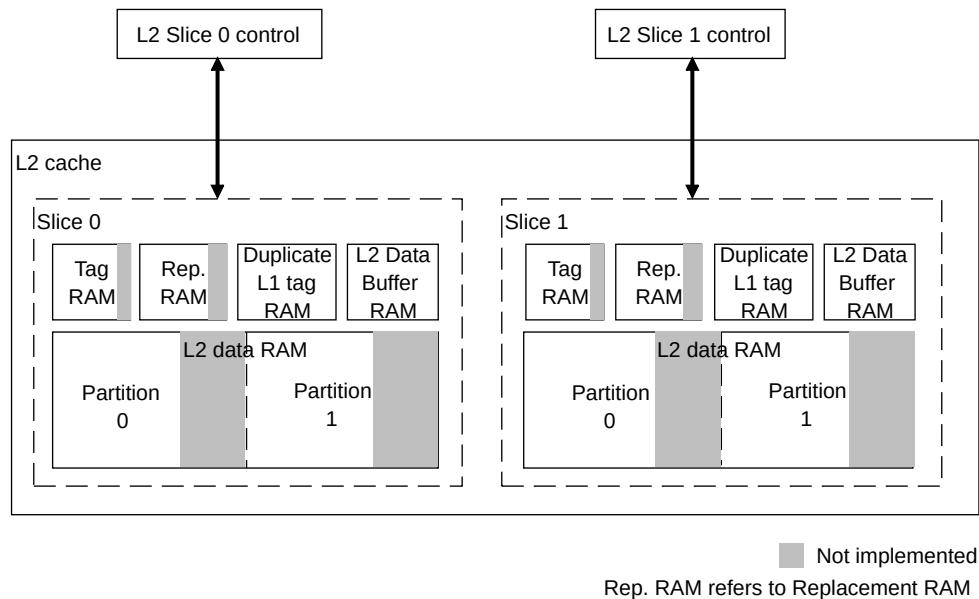
#### 8.4.1.2 Non-power-of-two L2 cache implementation

The Cortex®-R82AE processor supports the following non power-of-two L2 cache sizes: 96KB, 192KB, 384KB, 768KB, 1.5MB, 3MB.

When configured with a non power-of-two size, the number of L2 cache ways remains unchanged at 8 ways, but the overall number of sets is reduced compared to the equivalent power-of-two configuration.

The following figure shows a non power-of-two L2 cache implementation, highlighting the reduction in available sets across all slices and partitions when compared to the equivalent power-of-two size.



**Figure 8-3: Non-power-of-two L2 cache implementation**

### 8.4.2 L2 cache allocation policy

The L2 cache data allocation policy changes depending on the pattern of data usage.

Exclusive allocation is used when data is allocated in only one core. Inclusive allocation is used when data is shared between cores.

For example, an initial request from core 0 allocates data in the L1 caches but is not allocated in the L2 cache. When data is evicted from core 0, the evicted data is allocated in the L2 cache. The allocation policy of this cache line is still exclusive. If core 0 refetches the line, it is allocated in the L1 caches of core 0 and removed from the L2 cache, keeping the line exclusive. If core 1 then accesses the line for reading, it remains cached in core 0 and is also allocated in both core 1 and L2 caches. In this case, the line has inclusive allocation.

### 8.4.3 L2 cache partitioning

The L2 cache supports a partitioning scheme that alters the victim selection policy to prevent one core (or a group of cores) from using the entire cache at the expense of another core.

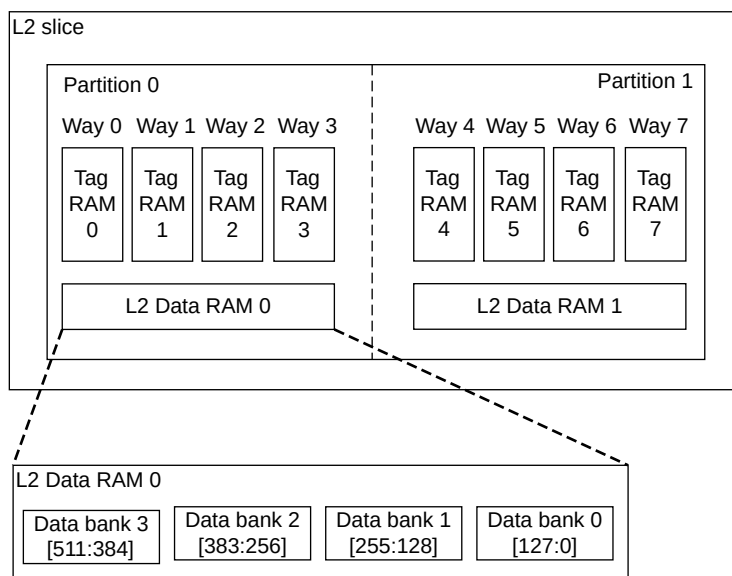
Cache partitioning is intended for specialized software where there are distinct classes of processes running with different cache accessing patterns. For example, two processes A and B run on

separate cores in the same cluster and therefore share the L2 cache. If process A is more data-intensive than process B, then process A can cause all the cache lines that process B allocates to be evicted. Evicting these allocated cache lines can reduce the performance of process B.

To avoid this, the Cortex®-R82AE processor supports L2 cache partitioning to enable differentiation between groups of cores with varying types of workload.

The L2 cache implements eight ways. When configured as a single slice, these all fall within a single partition, whereas a dual slice configuration implements four ways per partition as shown in the following figure.

**Figure 8-4: L2 cache slice structure**



To implement the cache way partitioning, the Cortex®-R82AE processor groups pairs of ways into Way Groups and associates these with the different cores via Scheme IDs.

The eight cache ways are arranged into groups as follows:

- Way Group 0: Way 0 and Way 4
- Way Group 1: Way 1 and Way 5
- Way Group 2: Way 2 and Way 6
- Way Group 3: Way 3 and Way 7

Eight combinations of these Way Groups can then be defined via the Cluster Partition Control Register, **IMP\_CLUSTERPARTCR\_EL1**. Each grouping is known as a Scheme ID. The Cluster Partition Control Register can be programmed as follows:

- Each way group can be assigned as private to one or more scheme IDs.
- Each way group can be left unassigned and therefore shared between all scheme IDs.

- Multiple way groups can be assigned as private to a single scheme ID.

These Scheme IDs can then be configured for use as follows:

- Each core is assigned to a scheme ID with the Cluster Scheme ID register, IMP\_CLUSTERSID\_EL1 which is banked per-core.
- *Main Accelerator Coherency Port* (MACP) transactions are assigned to a scheme ID with the Cluster MACP Scheme ID register IMP\_CLUSTERACPSID\_EL1.

Accesses from a given core or the MACP can allocate into any cache way that is assigned as private to the allocated Scheme ID, or to any cache way that is shared between all Scheme IDs.



If some cache ways are powered down, the number of ways in each partition are reduced. If there are insufficient ways available to a process, performance might be reduced. Therefore Arm recommends that using cache partitioning and cache way powerdown at the same time is done with care.

---

#### 8.4.4 L2 cache stashing

Cache stashing is the ability of an external agent to request that a line is brought in (or stashed) to a cache in the cluster.

Cache stashing can be performed over the *Main Accelerator Coherency Port* (MACP) or the *Main Manager* (MM) interface if it is configured as CHI. All stash requests target only the L2 cache.

Cache stashing is not supported on the *ACE-Lite Subordinate* (ACELS) interface or the MM interface if it is configured as AXI.

#### 8.4.5 L2 cache data RAM latency

The L2 cache data RAM input and output latency is configurable in order to meet a variety of potential frequency targets.

For more information on the L2 cache data RAM latency, see the *Arm® Cortex®-R82AE Configuration and Integration Manual*.



The *Arm® Cortex®-R82AE Configuration and Integration Manual* is a confidential document that is only available to Cortex®-R82AE processor IP licensees.

---

## 8.5 LLPP manager interface

The *Low-latency Peripheral Port* (LLPP) provides minimum latency access to memory and devices outside the cluster. Each core within the Cortex®-R82AE processor has an optional AXI5 32-bit LLPP manager interface.

The LLPP is expected to be connected to a limited number of latency-critical peripherals that are private to a core. No other core can access to the peripherals connected to a core's LLPP. Similarly, the *ACE-Lite Subordinate* (ACELS) interface cannot access to the LLPP.



Note

You can also connect the LLPP to a wider, shared interconnect, but its latency advantages would be reduced.

---

You can connect the LLPP to memory instead of peripherals although this is not optimal. This is because the LLPP always applies Device non-Gathering, non-Reordering, with no Early Write Acknowledgement (Device-nGnRnE) memory type and attributes. This means that the Cortex®-R82AE processor never speculatively accesses the LLPP, reorders accesses to the LLPP, forwards data from the LLPP, or merges writes to the LLPP.

Any accesses to the LLPP must follow the rules of the Device memory. The LLPP treats Normal memory accesses as if they are Device memory accesses.



Note

If you connect an ideal memory system to the LLPP, then the core can sustain one store word transaction (generated by basic STR instructions) each cycle to the LLPP indefinitely resulting a throughput of 32-bit of store data per cycle.

---

You can connect the LLPP to AXI4 subordinates, AXI5 subordinates, and AXI5-Lite subordinates.

The LLPP does not support exclusive or atomic transactions. Any exclusive or atomic accesses to the LLPP cause a synchronous External Data Abort that is generated internally rather than requiring the SoC to do so.

Unlike *Main Manager* (MM) accesses, the LLPP accesses are never shared or merged with accesses from a different context, even for Normal type memory. Therefore, it is always possible for the subordinate device to use the *Virtual Machine Identifier* (VMID) signaled on the LLPP to restrict accesses to a particular context.

The LLPP signals the VMID of the context that initiated a transaction on dedicated AXI User signals for all transactions. The LLPP supports only single-beat burst INCR transactions.

The IMP\_LLPPREGIONR\_EL1 System register holds the information about:

- Whether the LLPP is implemented or not.
- LLPP region size which is fixed to 128MB if the LLPP is implemented and 0 otherwise.

- The LLPP base address.
- Whether the LLPP is enabled or not.

LLPP configuration parameter controls whether the LLPP interface is implemented or not. If the system does not implement the LLPP interface ( $LLPP = 0$ ), the cores in the Cortex®-R82AE processor do not include the logic to support LLPP regions and ports. All related AXI signals, CFGLLPPIMP, and CFGLLPPBASEADDR pins are rendered out by the configuration script.

If the system implements the LLPP interface ( $LLPP = 1$ ), all cores in the Cortex®-R82AE processor include logic to support the LLPP regions and ports. The LLPP interfaces can be enabled or disabled by the CFGLLPPIMP pin. If the LLPP interface is implemented, the LLPP region has a fixed size of 128MB.

The LLPP base address is set via the configuration signal CFGLLPPBASEADDR and is the same for all cores in a cluster.

The LLPP is disabled at reset. IMP\_LLPPREGIONR\_EL1.ENABLEEL2 controls whether the LLPP is enabled for access at EL2 and IMP\_LLPPREGIONR\_EL1.ENABLEEL10 controls whether the LLPP is enabled for access at EL0 and EL1.

For more information about the IMP\_LLPPREGIONR\_EL1, see [A.2.2.41 IMP\\_LLPPREGIONR\\_EL1, LLPP Region Register](#) on page 535.

If the LLPP is implemented and enabled, data accesses to an address in the LLPP region are performed through the LLPP. If the LLPP is implemented and not enabled, data accesses to the LLPP region generate a synchronous External abort. If the LLPP is not implemented, then data accesses to the LLPP region are performed through other parts of the memory system.

If the LLPP is implemented, instruction accesses to an address in the LLPP region cause a synchronous External abort. If the LLPP is not implemented, instruction accesses are performed through other parts of the memory system.

The Cortex®-R82AE processor supports optional bus interface protection according to the AMBA® standard Data Check protocols on all signals for the LLPP. The Data Check protocols define parity bits for groups of signals, using odd parity.

The following table shows the LLPP attributes.

**Table 8-2: LLPP attributes**

Attribute	Value	Comments
Write issuing capability	8	Each core can issue a maximum of eight write requests.
Read issuing capability	4	Each core can issue a maximum of four LLPP read requests.
Combined issuing capability	12	Each core can issue a maximum of 12 requests.
Exclusive thread capability	0	Exclusive accesses are not supported.
Write ID capability	1	All writes use the same ID.
Write ID width	1	-
Read ID capability	1	All reads use the same ID.

Attribute	Value	Comments
Read ID width	1	-

### 8.5.1 LLPP features

The following table shows the *Low-latency Peripheral Port* (LLPP) AXI properties the Cortex®-R82AE processor supports or requires the cluster interconnect and system to support.

**Table 8-3: LLPP features**

AXI property	Supported by the Cortex®-R82AE processor LLPP	Interconnect support required
Continuous_Cache_Line_Read_Data	Not applicable	Yes
Multi_Copy_Atomicity	Yes	Yes
Ordered_Write_Observation	Yes	Yes
WriteEvict_Transaction	Yes if IMP_CLUSTERACTLR_EL1 Cache UniqueClean eviction control is programmed to 1.	Yes if IMP_CLUSTERACTLR_EL1 Cache UniqueClean eviction control is programmed to 1.
DVM_v8	Yes	Yes
Atomic_Transactions	No	No
DVM_v8.1	Yes	Yes if BROADCASTOUTERM is HIGH.
Poison	No	No
Check_Type	No if bus protection is not included (BUS_PROTECTION 0).  Odd_Parity_Byte_All if bus protection is included.	Yes
QoS_Accept	No	No
Trace_Signals	No	No
Loopback_Signals	No	No
Wakeup_Signals	Yes	Yes
Untranslated_Transactions	No	No
NSAccess_Identifiers	No	No

**Table 8-4: LLPP features**

AXI property	Supported by the Cortex®-R82AE processor LLPP	Interconnect support required
Multi_Copy_Atomicity	Yes	Yes
Ordered_Write_Observation	Yes	Yes
Atomic_Transactions	No	No
Poison	No	No
Check_Type	No	No
QoS_Accept	No	No
Trace_Signals	No	No

AXI property	Supported by the Cortex®-R82AE processor LLPP	Interconnect support required
Loopback_Signals	No	No
Wakeup_Signals	Yes	Yes
Untranslated_Transactions	No	No
NSAccess_Identifiers	No	No

## 8.5.2 LLPP memory attributes

The LLPP uses the ARCACHEPm and AWCACHEPm signals to indicate the memory attributes of transactions.

The following table shows the encoding that is used for the ARCACHEPm and AWCACHEPm signals of the LLPP manager interface. Because the LLPP is optimized for peripherals, all accesses propagate Device Non-bufferable attributes, regardless of the attributes that are returned by the memory management system translation. All other encodings are unused.

**Table 8-5: ARCACHEPm and AWCACHEPm encodings**

Encoding	Meaning
0b0000	Device Non-bufferable

## 8.5.3 LLPP transfers

The LLPP only issues INCR bursts of length one and transfers of up to 32 bits per transfer.

The LLPP read-channel can post:

- Two 32-bit outstanding transactions when a single instruction requests 64 bits of data from a 64-bit aligned location.
- Four 32-bit outstanding transactions when a single instruction requests 128 bits of data from a 128-bit aligned location.

The LLPP does not post two read transactions on the bus for two separate instructions or for data within two separate 64-bit aligned locations.

The LLPP write-channel generates up to eight 32-bit transactions on the bus from one or more instructions. All transactions use the same ID to ensure that ordering is maintained.

## 8.5.4 LLPP AXI transfer restrictions

The LLPP conforms to the AMBA® 5 AXI specification, but it does not generate all the AXI transaction types that the specification permits.

This section describes the types of AXI transactions that the LLPP generates. If you are designing an AXI Subordinate interface to work only with the Cortex®-R82AE LLPP, you can take advantage of these restrictions and the interface attributes to simplify the subordinate.

This section also contains tables that show some examples of the types of AXI burst that the Cortex®-R82AE processor generates. However, because a particular type of transaction is not shown here does not mean that the Cortex®-R82AE processor does not generate such a transaction.

You can connect the LLPP to both AXI4 subordinates and AXI5-Lite subordinates in addition to AXI5 subordinates.

An AXI4 subordinate device that is connected to the LLPP must be capable of handling every kind of transaction that the AXI4 specification permits, except where there is an explicit statement in this chapter that such a transaction is not generated. You must not infer any additional restrictions from the example tables given.

An AXI5-Lite subordinate device that is connected to the LLPP must be capable of handling every kind of transaction that the AXI5-Lite specification permits, except where there is an explicit statement in this chapter that such a transaction is not generated. You must not infer any additional restrictions from the example tables given.

Restrictions on AXI peripheral transfers describes restrictions on the type of transfers that the LLPP generates. If a core exists and is powered up, BREADYPm and RREADYPm are always asserted. You must not make any assumptions about the AXI handshaking signals, except that they conform to the AXI5 specification.

The LLPP applies the following restrictions to the AXI transactions it generates:

- A burst never transfers more than four bytes.
- The burst length is never more than one transfer.
- No transaction ever crosses a 4-byte boundary in memory.
- All transactions are incrementing (INCR) bursts.
- Transactions to Device memory are always to addresses that are aligned to the transfer size.
- No exclusive accesses are generated.
- No atomic accesses are generated.



### 8.5.4.1 LLPP Device transactions

This section details LLPP Device transactions.

The following table shows the values of ARADDRPm, ARBURSTPm, ARSIZEPm, and ARLENPm for `LDRB` from bytes 0-3 in Device memory.

**Table 8-6: `LDRB` transfers**

Address[1:0]	ARADDRPm[7:0]	ARBURSTPm	ARSIZEPm	ARLENPm
0x0 (byte 0)	0x00	INCR	8-bit	1 data transfer
0x1 (byte 1)	0x01	INCR	8-bit	1 data transfer
0x2 (byte 2)	0x02	INCR	8-bit	1 data transfer
0x3 (byte 3)	0x03	INCR	8-bit	1 data transfer

The following table shows the values of ARADDRPm, ARBURSTPm, ARSIZEPm, and ARLENPm for `LDRH` from halfwords 0-1 in Device memory.

**Table 8-7: `LDRH` transfers**

Address[1:0]	ARADDRPm	ARBURSTPm	ARSIZEPm	ARLENPm
0x0 (halfword 0)	0x00	INCR	16-bit	1 data transfer
0x2 (halfword 1)	0x02	INCR	16-bit	1 data transfer

The following table shows the values of ARADDRPm, ARBURSTPm, ARSIZEPm, and ARLENPm for an `LDR` that transfers a single word, `LDR <wt>`, in Device memory.

**Table 8-8: `LDR <wt>` transfers**

Address[1:0]	ARADDRPm	AWBURSTPm	ARSIZEPm	ARLENPm
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer

The following table shows the values of ARADDRPm, ARBURSTPm, ARSIZEPm, and ARLENPm for an `LDR` that transfers two 64-bit registers, an `LDR <xt>`, in Device memory.

All accesses using `LDR <xt>` instructions to Device memory occur as 32-bit transactions.

**Table 8-9: `LDR <xt>` transfers**

Address[3:0]	ARADDRPm	ARBURSTPm	ARSIZEPm	ARLENPm
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer

The following table shows the values of ARADDRPm, ARBURSTPm, ARSIZEPm, and ARLENPm for an `LDP` from words 0-1-2-3, in Device memory.

**Table 8-10: `LDP` transfers**

Address[3:0]	ARADDRPm	ARBURSTPm	ARSIZEPm	ARLENPm
0x0 (word 0)	0x00	INCR	8-bit	1 data transfer

Address[3:0]	ARADDRPm	ARBURSTPm	ARSIZEPm	ARLENPm
0x4 (word 1)	0x04	INCR	8-bit	1 data transfer
0x8 (word 2)	0x08	INCR	8-bit	1 data transfer
0xC (word 3)	0x0C	INCR	8-bit	1 data transfer

The following table shows the values of AWADDRPm, AWBURSTPm, AWSIZEPm, AWLENPm, and WSTRBPm for an **STRB** from bytes 0-3 in Device memory.

**Table 8-11: STRB transfers**

Address[1:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x0 (byte 0)	0x00	INCR	32-bit	1 data transfer	0b0001
0x1 (byte 1)	0x00	INCR	32-bit	1 data transfer	0b0010
0x2 (byte 2)	0x00	INCR	32-bit	1 data transfer	0b0100
0x3 (byte 3)	0x00	INCR	32-bit	1 data transfer	0b1000

The following table shows the values of AWADDRPm, AWBURSTPm, AWSIZEPm, AWLENPm, and WSTRBPm for an **STRH** from halfwords 0-1 in Device memory.

**Table 8-12: STRH transfers**

Address[1:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x0 (halfword 0)	0x00	INCR	32-bit	1 data transfer	0b0011
0x2 (halfword 1)	0x00	INCR	32-bit	1 data transfer	0b1100

The following table shows the values of AWADDRPm, AWBURSTPm, AWSIZEPm, AWLENPm, and WSTRBPm for an **STR** that writes a single word, **STR <wt>**, to Device memory.

**Table 8-13: STR <wt> transfers**

Address[1:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer	0b1111

The following table shows the values of AWADDRPm, AWBURSTPm, AWSIZEPm, AWLENPm, and WSTRBPm for an **STR** that transfers a 64-bit registers, an **STP <xt>**, to Device memory.

**Table 8-14: STR <xt> transfers**

Address[3:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer	0b1111
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer	0b1111

The following table shows the values of AWADDRPm, AWBURSTPm, AWSIZEPm, AWLENPm, and WSTRBPm for an **STP** that writes two 64-bit registers, an **STP <xt1>, <xt2>**, to Device memory.

**Table 8-15: STP transfers**

Address[3:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer	0b1111
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer	0b1111

Address[3:0]	AWADDRPm	AWBURSTPm	AWSIZEPm	AWLENPm	WSTRBPm
0x8 (word 2)	0x08	INCR	32-bit	1 data transfer	0b1111
0xC (word 3)	0x0C	INCR	32-bit	1 data transfer	0b1111



Note

- A load of a halfword from Device memory addresses 0x1 or 0x3 generates an alignment fault.
- A load of a word from Device memory addresses 0x1, 0x2, or 0x3 generates an alignment fault.
- A load-pair from Device memory addresses 0x1, 0x2, 0x3, 0x5, 0x6, or 0x7 generates an alignment fault.
- A store of a halfword from Device memory addresses 0x1, or 0x3 generates an alignment fault.
- A store of a word to Device memory addresses 0x1, 0x2, or 0x3 generates an alignment fault.
- A store-pair to Device memory address 0x1, 0x2, 0x3, 0x5, 0x6, or 0x7 generates an alignment fault.

## 8.6 SPP manager interface

The *Shared Peripheral Port* (SPP) provides minimum latency access to memory and devices outside the cluster. The Cortex®-R82AE processor has an optional AXI5 64-bit SPP manager interface that is shared among the cores within the cluster.

The SPP is expected to be connected to a limited number of latency-critical peripherals that are shared among cores. Each core can access to the peripherals connected to SPP. The *ACE-Lite Subordinate* (ACELS) interface cannot access to the SPP.



Note

You can also connect the SPP to a shared interconnect but its latency advantages would be reduced.

You can connect the SPP to memory instead of peripherals although this is not optimal. It is because the SPP always applies Device non-Gathering, non-Reordering, with no Early Write Acknowledgement (Device-nGnRnE) memory type and attributes. This means that the Cortex®-R82AE processor never speculatively accesses the SPP, reorders accesses to the SPP, forwards data from the SPP, or merges writes to the SPP. The SPP does not support exclusives and atomics.



Note

If you connect an ideal memory system to the SPP, then the Cortex®-R82AE processor sustains one store doubleword transaction (generated by basic STR

instructions) each cycle to the SPP indefinitely resulting a throughput of 64-bit of store data per cycle.

---

To guarantee the minimum latency characteristics of the SPP, you need to reserve certain buffers in the Cortex®-R82AE processor. For more information, see [8.15 Real-time considerations](#) on page 203.

You can connect the SPP to AXI4 subordinates, AXI5 subordinates, and AXI5-Lite subordinates. If you choose to connect the SPP to the AXI5-Lite subordinates, you must implement a bridge in your system to split the 2-beat bursts that SPP is capable of generating.

Unlike the *Main Manager* (MM) accesses, the SPP accesses are never shared or merged with accesses from a different context, even for Normal type memory. Therefore, it is always possible for the subordinate device to use the *Virtual Machine Identifier* (VMID) signaled on the SPP to restrict accesses to a particular context.

The SPP signals the VMID of the context that initiated a transaction on dedicated AXI User signals for all transactions to the SPP.

The SPP supports only INCR transactions and is capable of both single-beat and 2-beat bursts. For example, 128-bit load-store pair can be sent out as a 2-beat 64-bit INCR burst.

The SPP does not have exclusives or atomics support.

The IMP\_SPPREGIONR\_EL1 System register holds the information about:

- Whether the SPP is implemented or not.
- SPP region size which is fixed to 128MB if the SPP is implemented and 0 otherwise.
- The SPP base address.
- Whether the SPP is enabled or not.

SPP configuration parameter controls whether the SPP interface is implemented or not. If the system does not implement the SPP interface (SPP = 0), the Cortex®-R82AE processor does not include the SPP region and ports. All related AXI signals, CFGSPPIMP, and CFGSPPBASEADDR pins are rendered out by the configuration script.

If the system implements the SPP interface (SPP = 1), the Cortex®-R82AE processor includes the SPP region and ports. The SPP interface can be enabled or disabled by the CFGSPPIMP pin. If the SPP interface is implemented, the SPP region has a fixed size of 128MB.

The SPP base address is set via the configuration signal CFGSPPBASEADDR.

The SPP is disabled at reset. IMP\_SPPREGIONR\_EL1.ENABLEEL2 controls whether the SPP is enabled for access at EL2 and IMP\_SPPREGIONR\_EL1.ENABLEEL10 controls whether the SPP is enabled for access at EL0 and EL1.

For more information about the IMP\_SPPREGIONR\_EL1, see [A.2.2.43 IMP\\_SPPREGIONR\\_EL1, SPP Region Register](#) on page 540.

If the SPP is implemented and enabled, data accesses to an address in the SPP region are performed through the SPP. If the SPP is implemented and not enabled, data accesses to the SPP region generate a synchronous External abort. If the SPP is not implemented, then data accesses to the SPP region are performed through other parts of the memory system.

If the SPP is implemented, instruction accesses to an address in the SPP region cause a synchronous External abort. If the SPP is not implemented, instruction accesses are performed through other parts of the memory system.

The Cortex®-R82AE processor supports optional bus interface protection according to the AMBA® standard Data Check protocols on all signals for the SPP. The Data Check protocols define parity bits for groups of signals, using odd parity.

The following table shows SPP attributes where NUM\_CORES is the number of physical cores. See [1.3.1 Configuration parameters](#) on page 27 for permitted values.

**Table 8-16: SPP attributes**

Attribute	Value	Comments
Write issuing capability in SPLIT or HYBRID mode	NUM_CORES * 8	Each core can issue a maximum of eight write requests.
Write issuing capability in LOCK mode	NUM_CORES/2	Logical core.
Read issuing capability in SPLIT or HYBRID mode	NUM_CORES	Each core can issue one SPP read request.
Read issuing capability in LOCK mode	NUM_CORES/2	Logical core.
Combined issuing capability	NUM_CORES * 9	Each core can issue a maximum of nine requests with up to eight writes and one read.
Exclusive thread capability	0	No Exclusive access support.
Write ID capability	1 ID per core	All writes use the same ID per core. <b>Note:</b> Write ID capability is the same as the Read ID capability for the same core.
Write ID width	3 bits	Unused bits tied to zero if less than three bits required.
Read ID capability	1 ID per core	All reads use the same ID per core.
Read ID width	3 bits	Unused bits tied to zero if less than three bits required.

### 8.6.1 SPP features

The following table shows the *Shared Peripheral Port* (SPP) AXI properties the Cortex®-R82AE processor supports or requires the cluster interconnect and system to support.

**Table 8-17: SPP features**

AXI property	Supported by the Cortex®-R82AE processor SPP	Interconnect support required
Multi_Copy_Atomicity	Yes	Yes
Ordered_Write_Observation	Yes	Yes

AXI property	Supported by the Cortex®-R82AE processor SPP	Interconnect support required
Atomic_Transactions	No	No
Poison	No	No
Check_Type	No if bus protection is not included (BUS_PROTECTION 0).  Odd_Parity_Byte_All if bus protection is included.	Yes
QoS_Accept	No	No
Trace_Signals	No	No
Loopback_Signals	No	No
Wakeup_Signals	Yes	Yes
Untranslated_Transactions	No	No
NSAccess_Identifiers	No	No

## 8.6.2 SPP memory attributes

The Cortex®-R82AE processor does not implement AMBA® AXI5 ARCACHE and AWCACHE signals for the *Shared Peripheral Port* (SPP). The SPP uses the default values for these signals to indicate the memory attributes of transactions.

The following table shows the default encoding that is used for the ARCACHE and AWCACHE signals. Because the SPP is optimized for peripherals, all accesses propagate Device Non-bufferable attributes, regardless of the attributes that are returned by the memory management system translation. All other encodings are unused.

**Table 8-18: ARCACHE and AWCACHE encodings**

Encoding	Meaning
0b0000	Device Non-bufferable

## 8.6.3 SPP transfers

The SPP only issues INCR transactions of single-beat and 2-beat bursts and transfers of up to 128 bits per transfer.

The SPP read-channel can post one, up to 128-bit outstanding transaction per core when a single instruction requests 128 bits of data from a 128-bit aligned location. The SPP does not post two read transactions per core on the bus for two separate instructions.

The SPP write-channel generates up to eight write requests per core with up to 128-bit transactions on the bus from one or more instructions. All transactions use the same ID per core to ensure that ordering is maintained.

## 8.6.4 SPP AXI transfer restrictions

The SPP conforms to the AMBA® 5 AXI specification, but it does not generate all the AXI transaction types that the specification permits.

This section describes the types of AXI transactions that the SPP generates. If you are designing an AXI subordinate interface to work only with the Cortex®-R82AE SPP, you can take advantage of these restrictions and the interface attributes to simplify the subordinate.

This section also contains tables that show some examples of the types of AXI burst that the Cortex®-R82AE processor generates. However, because a particular type of transaction is not shown here does not mean that the Cortex®-R82AE processor does not generate such a transaction.

You can connect the SPP to both AXI4 subordinates and AXI5-Lite subordinates in addition to AXI5 subordinates.

An AXI4 subordinate device that is connected to the SPP must be capable of handling every kind of transaction that the AXI4 specification permits, except where there is an explicit statement in this chapter that such a transaction is not generated. You must not infer any additional restrictions from the example tables given.

An AXI5-Lite subordinate device that is connected to the SPP must be capable of handling every kind of transaction that the AXI5-Lite specification permits, except where there is an explicit statement in this chapter that such a transaction is not generated. You must not infer any additional restrictions from the example tables given.



If you connect the SPP to AXI5-Lite subordinates, then you must implement a bridge in your system to split the 2-beat bursts that SPP is capable of generating.

---

Restrictions on AXI peripheral transfers describes restrictions on the type of transfers that the SPP generates. You must not make any assumptions about the AXI handshaking signals, except that they conform to the AXI5 specification.

The SPP applies the following restrictions to the AXI transactions it generates:

- A burst never transfers more than 16 bytes.
- The burst length is never more than two transfers.
- No transaction ever crosses a 16-byte boundary in memory.
- All transactions are incrementing (INCR) bursts.
- Transactions to Device memory are always to addresses that are aligned to the transfer size (not to the transaction size).
- Does not support exclusive accesses and atomics.

### 8.6.4.1 SPP transactions

This section describes the Cortex®-R82AE processor *Shared Peripheral Port* (SPP) transactions. The SPP Device memory and Normal memory transactions are the same.

The following table shows the values of ARADDRD, ARBURSTD, ARSIZED, and ARLEND for `LDRB` from bytes 0-7.

**Table 8-19: LDRB transfers**

Address[2:0]	ARADDRD	ARBURSTD	ARSIZED	ARLEND
0x0 (byte 0)	0x00	INCR	8-bit	1 data transfer
0x1 (byte 1)	0x01	INCR	8-bit	1 data transfer
0x2 (byte 2)	0x02	INCR	8-bit	1 data transfer
0x3 (byte 3)	0x03	INCR	8-bit	1 data transfer
0x4 (byte 4)	0x04	INCR	8-bit	1 data transfer
0x5 (byte 5)	0x05	INCR	8-bit	1 data transfer
0x6 (byte 6)	0x06	INCR	8-bit	1 data transfer
0x7 (byte 7)	0x07	INCR	8-bit	1 data transfer

The following table shows the values of ARADDRD, ARBURSTD, ARSIZED, and ARLEND for `LDRH` from halfwords 0-3.

**Table 8-20: LDRH transfers**

Address[2:0]	ARADDRD	ARBURSTD	ARSIZED	ARLEND
0x0 (halfword 0)	0x00	INCR	16-bit	1 data transfer
0x2 (halfword 1)	0x02	INCR	16-bit	1 data transfer
0x4 (halfword 2)	0x04	INCR	16-bit	1 data transfer
0x6 (halfword 3)	0x06	INCR	16-bit	1 data transfer

The following table shows the values of ARADDRD, ARBURSTD, ARSIZED, and ARLEND for an `LDR` transfer.

**Table 8-21: LDR transfers**

Address[2:0]	ARADDRD	AWBURSTD	ARSIZED	ARLEND
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer
0x0 (doubleword 0)	0x00	INCR	64-bit	1 data transfer

The following table shows the values of ARADDRD, ARBURSTD, ARSIZED, and ARLEND for an `LDP`.

All accesses using `LDP` instructions to memory occur as one or multiple 32-bit transactions or one or multiple 64-bit transactions.



**Table 8-22: LDP transfers for two 32-bit registers**

Address[2:0]	ARADDRD	ARBURSTD	ARIZED	ARLEND
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer
	0x04	INCR	32-bit	1 data transfer
	0x08	INCR	32-bit	1 data transfer
	0x0C	INCR	32-bit	1 data transfer
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer
	0x08	INCR	32-bit	1 data transfer
	0x0C	INCR	32-bit	1 data transfer

**Table 8-23: LDP transfers for two 64-bit registers**

Address[2:0]	ARADDRD	ARBURSTD	ARIZED	ARLEND
0x0 (quadword)	0x00	INCR	64-bit	2 data transfers

The following table shows the values of AWADDRD, AWBURSTD, AWSIZED, AWLEND, and WSTRBD for an STRB from bytes 0-7 in memory.

**Table 8-24: STRB transfers**

Address[2:0]	AWADDRD	AWBURSTD	AWSIZED	AWLEND	WSTRBD
0x0 (byte 0)	0x00	INCR	8-bit	1 data transfer	0b00000001
0x1 (byte 1)	0x01	INCR	8-bit	1 data transfer	0b00000010
0x2 (byte 2)	0x02	INCR	8-bit	1 data transfer	00000b0100
0x3 (byte 3)	0x03	INCR	8-bit	1 data transfer	0b00001000
0x4 (byte 4)	0x04	INCR	8-bit	1 data transfer	0b00010000
0x5 (byte 5)	0x05	INCR	8-bit	1 data transfer	0b00100000
0x6 (byte 6)	0x06	INCR	8-bit	1 data transfer	0b01000000
0x7 (byte 7)	0x07	INCR	8-bit	1 data transfer	0b10000000

The following table shows the values of AWADDRD, AWBURSTD, AWSIZED, AWLEND, and WSTRBD for an STRB from halfwords 0-3 in memory.

**Table 8-25: STRH transfers**

Address[2:0]	AWADDRD	AWBURSTD	AWSIZED	AWLEND	WSTRBD
0x0 (halfword 0)	0x00	INCR	16-bit	1 data transfer	0b00000011
0x2 (halfword 1)	0x02	INCR	16-bit	1 data transfer	0b00001100
0x4 (halfword 2)	0x04	INCR	16-bit	1 data transfer	0b00110000
0x6 (halfword 3)	0x06	INCR	16-bit	1 data transfer	0b11000000

The following table shows the values of AWADDRD, AWBURSTD, AWSIZED, AWLEND, and WSTRBD for an STR to memory.

**Table 8-26: STR transfers**

Address[2:0]	AWADDRD	AWBURSTD	AWSIZED	AWLEND	WSTRBD
0x0 (word 0)	0x00	INCR	32-bit	1 data transfer	0b00001111
0x4 (word 1)	0x04	INCR	32-bit	1 data transfer	0b11110000
0x0 (doubleword 0)	0x00	INCR	64-bit	1 data transfer	0b11111111

The following table shows the values of AWADDRD, AWBURSTD, AWSIZED, AWLEND, and WSTRBD for an STR that writes two 64-bit registers, an STR <xt1>, <xt2>, to memory.

**Table 8-27: STP transfers for two 64-bit registers**

Address[2:0]	AWADDRD	AWBURSTD	AWSIZED	AWLEND	WSTRBD
0x0 (quadword)	0x00	INCR	64-bit	2 data transfer	0b11111111
					0b11111111

The following table shows the values of AWADDRD, AWBURSTD, AWSIZED, AWLEND, and WSTRBD for an STP that writes two 32-bit registers, an STP <Rt1>, <Rt2>, to memory.

**Table 8-28: STP transfers for two 32-bit registers**

Address[2:0]	AWADDRD	AWBURSTD	AWSIZED	AWLEND	WSTRBD
0x0	0x00	INCR	64-bit	1 data transfer	0b11111111
0x4	0x04	INCR	32-bit	2 data transfer	0b11110000
0x6					0b00001111

For the *Shared Peripheral Port* (SPP) transactions:

- A load of a halfword from memory addresses 0x1 or 0x3 generates an alignment fault.
- A load of a word from memory addresses 0x1, 0x2, or 0x3 generates an alignment fault.
- A load of a doubleword from memory addresses 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, or 0x7 generates an alignment fault.
- A 32-bit load-pair from memory addresses 0x1, 0x2, 0x3, 0x5, 0x6, or 0x7 generates an alignment fault.
- A 64-bit load-pair from memory addresses 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, or 0x7 generates an alignment fault.
- A store of a halfword from memory addresses 0x1, or 0x3 generates an alignment fault.
- A store of a word to memory addresses 0x1, 0x2, or 0x3 generates an alignment fault.
- A store of a doubleword from memory addresses 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, or 0x7 generates an alignment fault.
- A 32-bit store-pair to memory address 0x1, 0x2, 0x3, 0x5, 0x6, or 0x7 generates an alignment fault.



Note

- A 64-bit store-pair to memory address 0x1, 0x2, 0x3, 0x4 0x5, 0x6, or 0x7 generates an alignment fault.
- 

## 8.7 MM interface

The *Main Manager* (MM) interface is the default memory interface of the Cortex®-R82AE processor. The MM interface is optimized for highest average performance for contexts where determinism is less critical. However, a real-time context is also able to access the MM port, although such an access might not be desirable depending on the system design.

The MM interface is used for all the memory space that is not associated with another interface.

The MM interface is used for accesses to high-latency memory such as DDR and non-critical peripherals that are shared between cores within the cluster and other agents in the system.

You are expected to connect the MM port to an interconnect.

You can configure the MM port as:

- A 256-bit AMBA® CHI.E requester that can be connected to a CHI.E subordinate.
- A 256-bit AMBA® 5 AXI manager interface that can be connected to either an AMBA® 4 AXI or an AMBA® 5 AXI subordinate interface.

The MM port is accessible by external agents through the *Main Accelerator Coherency Port* (MACP) subordinate interface.

Accesses to the MM port can be cached in both the L1 (data caches and instruction caches) and L2 cache as determined by memory type and attributes. The Cortex®-R82AE processor supports only Write-Back caching of MM addresses. MM addresses that are marked as Write-Through cacheable are treated as Non-cacheable.

The Cortex®-R82AE processor includes hardware coherency logic for addresses in the MM address ranges so that software does not need to maintain cache coherency for shared data. The Cortex®-R82AE processor coherency hardware automatically updates the contents of L1 data and L2 caches within the cluster to ensure all cores within the cluster have the same coherent view of memory (full coherency).

The coherency hardware also provides coherency with non-cached external agents accessing the MM port through the MACP subordinate interface. The coherency hardware automatically updates the contents of caches within the cluster but is not able to update the content of managers connected to the MACP (I/O coherency).

When the MM port is configured as a CHI requester, the coherency hardware also provides coherency with external coherent agents connected through a coherent interconnect. The coherency hardware automatically processes CHI coherency requests and update the contents of caches within the cluster. The coherency hardware also generates CHI coherency requests on the MM port for the coherent system to process.

When configured as a CHI requester, the Cortex®-R82AE processor MM interface accepts and processes stashing requests to the L2 cache. This enables an external coherent requester to request the Cortex®-R82AE processor to fetch a cache line on the MM port and allocate it in the L2 cache.

The Cortex®-R82AE processor MM interface supports atomic instructions and performs all the atomics either in the L1 data cache or in the interconnect outside the Cortex®-R82AE processor if the interconnect supports the atomics.

The Cortex®-R82AE processor does not include logic to perform atomic operations at the cluster level. Whether the atomic instructions are handled within the core or atomic transactions are generated on the MM port depends on:

- The memory shareability attributes.

This allows you to design systems where:

- Atomic transactions are generated on the MM if BROADCASTATOMIC is set to 0
- Atomic transactions are generated on the MM and the Cortex®-R82AE processor cluster is just one of the number of agents accessing a shared location.

### 8.7.1 CHI requester interface

You can configure the Cortex®-R82AE processor to use the AMBA® 5 CHI protocol for the *Main Manager* (MM) interface.

The Cortex®-R82AE processor supports CHI Issue E.

#### 8.7.1.1 CHI features

AMBA® defines a set of interface properties for the CHI interconnect. The following table shows which of these properties the Cortex®-R82AE processor supports, or requires the interconnect and system to support.

#### 8.7.1.2 CHI configurations

You can change the coherency configurations to suit your system configuration using the BROADCASTCACHEMAINTM and BROADCASTOUTERM input signals.

#### CHI configurations

The following table shows the permitted combinations of these signals and the supported configurations in the Cortex®-R82AE processor with a CHI bus.

**Table 8-29: Supported CHI configurations**

Signal	Feature			
	CHI non-coherent		CHI coherent	
	With no cache or invisible system cache	With visible system cache	With invisible system cache	With visible system cache
BROADCASTCACHEMAINTM	0	1	0	1
BROADCASTOUTERM	0	0	1	1
BROADCASTPERSISTM	0	1	0	1 <b>Note:</b> BROADCASTOUTERM should be set or BROADCASTCACHEMAINTM should be set. Or BROADCASTPERSISTM and a CleanSharedPersist.
BROADCASTATOMICM	0	1	0	1
BROADCASTICINVALM	0	1	0	1 <b>Note:</b> Blocks IC DVMs from going external.
BROADCASTTLBIINNERM	0	1	0	1
BROADCASTTLBIOUTERM	0	1	0	1

**Note**

- A visible system cache requires cache maintenance transactions to ensure that a write is visible to all observers.
- An invisible system cache is one that does not require cache maintenance transactions to ensure that a write is visible to all observers. This is true even if those observers use different memory attributes.

The following table shows the key features in each of the supported CHI configurations.

**Table 8-30: Supported features in the CHI configurations**

Features	Configuration		
	CHI non-coherent		CHI coherent
	With no cache or invisible system cache	With visible system cache	
Cache maintenance requests on TXREQ channel	No	Yes	Yes
Snoops on RXSNP channel	No	No	Yes
Coherent requests on TXREQ channel	No	No	Yes
DVM requests on TXREQ channel	No	No	Yes

The input signals BROADCASTTLBIINNER and BROADCASTTLBIOUTER control the broadcasting of *TLB Invalidate* (TLBI) DVM messages to the external interconnect. The following table shows how the broadcast of the TLBI messages are controlled for the Inner and Outer Shareable domains depending on the configuration of BROADCASTTLBIINNER and BROADCASTTLBIOUTER.

**Table 8-31: Control of Inner and Outer Shareable TLBI messages to the external interconnect**

BROADCASTTLBIINNER	BROADCASTTLBIOUTER	Description
LOW	LOW	No TLBI transactions are broadcast outside the cluster
LOW	HIGH	Outer Shareable TLBI transactions, TLBI {OS}, generate TLBI transactions that are broadcast from the cluster. No other TLBI instructions generate TLBI transactions that are broadcast from the cluster.
HIGH	LOW	Invalid configuration
HIGH	HIGH	Inner shareable TLBI instructions, TLBI {IS}, and Outer shareable TLBI instructions, TLBI {OS}, generate TLBI transactions that are broadcast from the cluster.

### Cluster Power Mode Blocking

It should be noted that tying the CHI RXSACTIVE signal high then it may not be possible for the cluster to enter a lower power mode, for example, ON to OFF or ON to MEM\_RET. A stream of external snoop requests can also prevent a power transition to a lower power mode from completing until the stream of external snoops and outstanding snoops have completed.

#### 8.7.1.3 CHI requester interface attributes

The following table lists the possible values for the read and write issuing capabilities.

**Table 8-32: Attributes of the CHI requester interface**

Attribute	Value	Comments
Write issuing capability	Configuration dependent	The maximum number of writes is: <ul style="list-style-type: none"> <li>26, if L2_SLICES = 1.</li> <li>52, if L2_SLICES = 2</li> </ul>
Read issuing capability	Configuration dependent	The maximum number of reads is: <ul style="list-style-type: none"> <li><math>(\text{NUM\_CPUS} * 8) + (16 * \text{L2\_SLICES})</math> if L2 cache is not implemented</li> <li><math>(\text{NUM\_CPUS} * 10) + (16 * \text{L2\_SLICES})</math> if L2 cache is implemented</li> </ul> <p><b>Note:</b> Two-part Distributed Virtual Memory (DVM) messages use the same ID for both parts, and therefore can have two outstanding transactions on the same ID.</p> <p><b>Note:</b> In some cases, the L2 cache may be able to exceed this read acceptance capability. However this is rare and should not be used when sizing your interconnect.</p>
Exclusive hardware access thread capability	Number of hardware threads.	Each hardware thread can have one exclusive access sequence in progress.

Attribute	Value	Comments
Transaction ID width	12 bits	There is no fixed mapping between CHI transaction IDs and cores. Transaction IDs can be used for either reads or writes. <b>Note:</b> The source of the transaction is encoded in the LPID field, see <a href="#">Table 8-34: CHI LPID assignment</a> on page 165.
Transaction ID capability	Configuration dependent	The ID capability is: <ul style="list-style-type: none"> <li><math>(\text{NUM\_CPUS} * 8) + (16 * \text{L2\_SLICES})</math> if L2 cache is not implemented</li> <li><math>(\text{NUM\_CPUS} * 10) + (16 * \text{L2\_SLICES})</math> if L2 cache is implemented</li> </ul> <b>Note:</b> Unlike in an AMBA® ACE5 configuration, there is never any ID reuse in CHI implementations, regardless of the memory type.
NodeID widths	11 bits	-
TXREQFLITM.RSVDC	0 bits	-
TXDATFLITM.RSVDC	0 bits	-
TXDATFLITM.DataCheck	0 bits	-

**Note**

The issuing capability described here is the maximum for the whole cluster, and can be used to size interconnect capabilities if you want to achieve the maximum performance available. However a single core may not reach this maximum on its own. It may need multiple cores generating heavy memory traffic simultaneously to reach maximum performance. The capabilities vary by memory type, with typically a significantly lower limit for Device or Non-cacheable transactions than for Cacheable transactions.

#### 8.7.1.4 CHI channel properties

The following table shows the snoop capabilities and other CHI channel properties for the Cortex®-R82AE processor.

**Table 8-33: CHI channel properties**

Property	Value	Comment
Snoop acceptance capability	Configuration dependent	The L2 coherency logic can accept and process a maximum of 9 snoop requests from the system.
DVM acceptance capability	4	<p>The L2 coherency logic can accept and process a maximum of four <i>Distributed Virtual Memory</i> (DVM) transactions from the system. Each of these four transactions can be a two part DVM message.</p> <p>The interconnect must be configured to never send more than four DVM messages to the cluster, otherwise the system might deadlock.</p>

Property	Value	Comment
Snoop latency	Hit	When there is a hit in L2 cache, the best case for response and data is 10 SCLK cycles. When there is a miss in the L2 cache but a hit in an L1 cache in a core, then the latency varies. This latency variation depends on the type and configuration of that core.  Latencies can be higher if hazards occur or if there are not enough buffers to absorb requests.
	Miss	Best case for latency is six SCLK cycles when the snoop filter and L2 cache tags indicate the miss.
	DVM	The cluster takes a minimum of six SCLK cycles to provide a response to DVM packets.
Snoop filter	Supported	The cluster provides support for an external snoop filter in an interconnect. It indicates when clean lines are evicted from the cluster by sending Evict transactions on the CHI write channel.  However there are some cases that can prevent an Evict transaction from being sent. Therefore you must ensure that you build any external snoop filter to handle a capacity overflow. When exceeding capacity, the snoop filter should send a back-invalidation to the cluster.  Examples of case where evicts are not produced include: <ul style="list-style-type: none"> <li>• Linefills that take External aborts.</li> <li>• Store exclusives that fail.</li> <li>• Mis-matched aliases.</li> </ul>
Supported transactions	-	All transactions that are described by the CHI protocol: <ul style="list-style-type: none"> <li>• Are accepted on the CHI requester interface from the system.</li> <li>• Can be produced on the CHI requester interface except: <ul style="list-style-type: none"> <li>◦ ReadShared.</li> <li>◦ MakeInvalid.</li> <li>◦ EOBarrier.</li> <li>◦ ECBarrier.</li> <li>◦ WriteCleanPtl.</li> <li>◦ WriteUniquePtl.</li> <li>◦ WriteBackPtl.</li> <li>◦ WriteUniqueFullStash.</li> <li>◦ WriteUniquePtlStash.</li> <li>◦ ReadOnceCleanInvalid.</li> <li>◦ ReadOnceMakeInvalid.</li> </ul> </li> </ul>

### 8.7.1.5 CHI transactions

CHI transactions are sent to a specific node in the interconnect that is based on the following criteria:

- Type of access.
- Address of the access.
- Settings of the System Address Map.



Addresses that map to an HN-F node can be marked as cacheable memory in the translation tables, and can take part in the cache coherency protocol. Addresses that map to an HN-I or MN must be marked as device or Non-cacheable memory.

CHI TXREQ transactions include the *Logical Processor ID* (LPID) field. This field uniquely identifies the logical core that generated the request transaction. The following table shows CHI LPID assignment.

**Table 8-34: CHI LPID assignment**

LPID	Description
0x00-0x07	CPUID
0x08	ACP request.

**Table 8-35: CHI transaction types**

Transaction	Operation
ReadNoSnp	Non-cacheable loads or instruction fetches. Linefills of Non-shareable cache lines into L1 or L2 caches.
ReadOnce	Cacheable loads that are not allocating into the cache.
ReadNotSharedDirty	Cache data linefills started by a load instruction, or cache linefills started by an instruction fetch.
ReadUnique	Cache data linefills started by a store instruction.
CleanUnique	Store instructions that hit in the cache but the line is not in a unique coherence state.
MakeUnique	Store instructions of a full cache line of data, that miss in the caches.
MakeReadUnique	Read request to a Snoopable address region requesting a unique copy of a cache line.
CleanShared	Cache maintenance instructions.
CleanSharedPersistSep	Cache maintenance instructions. This is only generated by the <i>Data Cache Clean to the Point of Persistence</i> (DC_CVAP) cache maintenance instruction when the BROADCASTPERSISTM input signal is HIGH.
CleanInvalid	Cache maintenance instructions.
DVMOp	TLB and instruction cache maintenance instructions.
EOBarrier	Not used.
ECBarrier	Not used.
PrefetchTgt	Hardware prefetch hint to the memory controller.
StashOnceShared	Cache prefetch when there is no L2 cache present.
StashOnceUnique	Cache prefetch when there is no L2 cache present.
WriteNoSnpPtl	Non-cacheable store instructions.
WriteNoSnpFull	Non-cacheable store instructions, or evictions of Non-shareable cache lines.
WRITENOSNPCLEANSHARED	Combined WRITENOSNP with CleanShared CMO.
WRITENOSNPCLEANINVALID	Combined WRITENOSNP with CleanInvalid CMO.
WriteUniqueFull	Cacheable writes of a full cache line, that are not allocating into L1 or L2 caches, for example streaming writes.
WriteUniquePtl	Not used.
WriteBackFull	Evictions of dirty lines from the L1 or L2 caches.
WRITEBACKFULLCLEANINVALID	Combined WRITEBACKFULL with CLEANINVALID CMO
WriteBackPtl	Not used.

Transaction	Operation
WriteCleanFull	Evictions of dirty lines from the L2 cache, when the line is still present in an L1 cache. Some cache maintenance instructions.
WRITECLEANFULLCLEANSHARED	Combined WRITECLEANFULL with CLEANSHARED CMO.
WriteCleanPtl	Not used.
WriteEvictFull	Evictions of unique clean lines, when configured in the IMP_CLUSTERACTLR_EL1.
WRITEEVICTOREVICT	WriteBack of Clean data to the next-level cache. This request type is merging of WriteEvictFull and Evict into one request.
Evict	Evictions of clean lines, when configured in the IMP_CLUSTERACTLR_EL1.
AtomicStore	Atomic instruction.
AtomicLoad	Atomic instruction.
AtomicSwap	Atomic instruction.
AtomicCompare	Atomic instruction.
WriteUniqueFullStash	Not used.
WriteUniquePtlStash	Not used.
ReadOnceCleanInvalid	Not used.
ReadOnceMakeInvalid	Not used.

External memory accesses generate the following transactions in an implementation configured with a CHI requester interface.

**Table 8-36: CHI transaction usage**

Attributes		CHI transaction				
Memory type	Shareability	SnpAttr	Load	Store	Load exclusive	Store exclusive
Device.	Outer Shareable	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp and Excl set to HIGH.	WriteNoSnp and Excl set to HIGH.
Normal, Inner Non-cacheable, Outer Non-cacheable.	Non-shareable	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp and Excl set to HIGH.	WriteNoSnp and Excl set to HIGH.
	Inner Shareable					
	Outer Shareable					
Normal, Inner Non-cacheable, Outer Write-Back or Write-Through, or Normal, Inner Write-Through, Outer Write-Back, Write-Through or Non-cacheable, or Normal Inner Write-Back Outer Non-cacheable or Write-Through.	Non-shareable	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp and Excl set to HIGH.	WriteNoSnp and Excl set to HIGH.
	Inner Shareable					
	Outer Shareable					
Normal, Inner Write-Back, Outer Write-Back.	Non-shareable	Non-snoopable	ReadNoSnp	WriteNoSnp when the line is evicted or if not allocating into the cache.	ReadNoSnp	WriteNoSnp when the line is evicted.

Attributes		CHI transaction				
Memory type	Shareability	SnpAttr	Load	Store	Load exclusive	Store exclusive
	Inner Shareable	Snoopable	ReadNotSharedDirty	ReadUnique, CleanUnique, or MakeUnique if allocating into the cache, then a WriteBackFull when the line is evicted.  WriteUniqueFull if not allocating into the cache.	ReadNotSharedDirty, with Excl set to HIGH.	CleanUnique with Excl set to HIGH if required, then a WriteBackFull when the line is evicted.
	Outer Shareable	Snoopable				

### 8.7.1.6 Use of DataSource

Some CHI responses from the interconnect include a DataSource field indicating where the data was supplied from.

When making use of the DataSource field, Arm recommends providing this information as accurately as possible using the encodings recommended in the table *Suggested DataSource value encodings* provided in the [AMBA® CHI Architecture Specification](#).

The value of this field is used to calculate some *Performance Monitoring Unit* (PMU) events. It can also be used by some processors to tune the performance of their data prefetchers.

### 8.7.1.7 Support for memory types

The Cortex®-R82AE processor simplifies the coherency logic by downgrading some memory types.

Normal memory that is marked as both Inner Write-Back Cacheable and Outer Write-Back Cacheable is cached in the core data caches and the L2 cache.

All other Normal memory types are treated as Non-cacheable and are sent on the MM bus interface as Normal Non-cacheable.

## 8.7.2 AXI manager interface

The AXI *Main Manager* (MM) port is a 256-bit AMBA® 5 AXI manager that can be connected to either an AMBA® 4 AXI or an AMBA® 5 AXI subordinate interface.

When configured as an AXI manager, the MM port implements the following signals that are specified in AXI5 but not in AXI4:

- Signal integrity protection signals. These signals are intended to provide point-to-point protection between the Cortex®-R82AE processor cluster and the interconnect and can be transmitted through Data Check signals.
- Atomic operation signal, BROADCASTATOMICM. This signal is used to enable or disable broadcasting of atomic instructions on the MM interface.
- This can be achieved by tying CFGMMPOISON to 0 during the integration of the Cortex®-R82AE processor into your system. From the Cortex®-R82AE processor register definition, when such field is set to 0 Main Manager port does not support poison.

The MM port implements the atomic operation signal, BROADCASTATOMICM, that is specified in AXI5 but not in AXI4. This signal is used to enable or disable broadcasting of atomic instructions on the MM interface.

The Cortex®-R82AE processor includes coherency hardware that automatically manages the contents of caches within the cluster to ensure all cores have a coherent view of AXI MM addresses.

When configured as an AXI manager, the MM port does not support:

- Barriers on AR and AW channels.
- Cache maintenance requests on AR channel.
- Snoop capabilities.

### 8.7.2.1 MM AXI features

AMBA® defines a set of interface properties for the AXI interconnect. The following table shows which of these properties the Cortex®-R82AE processor *Main Manager* (MM) interface supports or requires the cluster interconnect and system to support.

**Table 8-37: AXI interconnect properties for the Cortex®-R82AE processor**

AXI property	Supported by the Cortex®-R82AE processor MM	Interconnect support required
Multi_Copy_Atomicity	Yes	Yes
Ordered_Write_Observation	Yes	Yes
Atomic_Transactions	Yes	Yes
Poison	Yes	Yes
Check_Type	No if bus protection is not included (BUS_PROTECTION 0).  Odd_Parity_Byte_All if bus protection is included.	Yes
QoS_Accept	No	No
Trace_Signals	No	No
Loopback_Signals	No	No
Wakeup_Signals	Yes	Yes

AXI property	Supported by the Cortex®-R82AE processor MM	Interconnect support required
Untranslated_Transactions	No	No
NSAccess_Identifiers	No	No

### 8.7.2.2 MM AXI attributes

The following table lists the read and write issuing capabilities for the *Main Manager* (MM) AXI interface.

**Table 8-38: AXI manager interface attributes**

Attribute	Value	Comments
Write issuing capability	Configuration dependent	The maximum number of writes is: <ul style="list-style-type: none"> <li>13, if the L2 is configured with a single slice</li> <li>26, if configured with two slices</li> </ul>
Read issuing capability	<ul style="list-style-type: none"> <li>(NUM_CORES * 8) + 4, if L2 cache is not implemented</li> <li>(NUM_CORES * 10) + 4, if L2 cache is implemented</li> </ul>	<p>The maximum number of reads is:</p> <ul style="list-style-type: none"> <li>68 if L2 cache is not implemented</li> <li>84 if L2 cache is implemented</li> </ul> <p><b>Note:</b> Two-part <i>Distributed Virtual Memory</i> (DVM) messages use the same ID for both parts, and therefore can have two outstanding transactions on the same ID.</p> <p><b>Note:</b> In some cases, the L2 cache may be able to exceed this read acceptance capability. However this is rare and should not be used when sizing your interconnect.</p>
Combined issuing capability	Configuration dependent (NUM_CORES and L2 cache implemented or not)	The maximum combined issuing capability is 116 (Eight cores and L2 cache implemented).
Exclusive thread capability	Number of hardware threads, maximum eight threads (one per core)	Each hardware thread can have one exclusive access sequence in progress.
Write ID capability	Configuration dependent	<p>The maximum write ID capability is:</p> <ul style="list-style-type: none"> <li>57, if less than four cores are present.</li> <li>89, if four or more cores are present.</li> </ul> <p>Only Device memory types with nGnRnE or nGnRE can have more than one outstanding transaction with the same AXI ID. All other memory types use a unique AXI ID for every outstanding transaction.</p>
Write ID width	13	The ID encodes the source of the memory transaction. See the Encodings for AWIDM[12:0] table.

Attribute	Value	Comments
Read ID capability	Configuration dependent	<p>The maximum read ID capability is:</p> <ul style="list-style-type: none"> <li>185, if less than four cores are present.</li> <li>345, if four or more cores are present.</li> </ul> <p>Only Device memory types with nGnRnE or nGnRE can have more than one outstanding transaction with the same AXI ID. All other memory types use a unique AXI ID for every outstanding transaction.</p> <p>Two part DVMs use the same ID for both parts, and therefore can have two outstanding transactions on the same ID.</p>
Read ID width	13	The ID encodes the source of the memory transaction. See the Encodings for ARIDM[12:0] table.



The issuing capability described here is the maximum possible for the whole cluster. This can be used to size interconnect capabilities if you want to achieve the maximum performance available. However, this maximum may not be reached depending on the Cortex®-R82AE processor configuration and characteristics of your system.

The following table shows the encodings for AWIDM[12:0], ARIDM[12:0].

**Table 8-39: Encodings for AWIDM[12:0]**

Attribute	Value	Issuing capability per ID	Description	Comments
Write ID	0b00nnn00000000	1	System domain store exclusives, excluding Device non-Reordering	nnn = Core ID
	0b11ssss0000000	15	Non-Reordering Device writes	ssss = Subordinate ID
	0b10nnncr0ammmm	1	All other writes	<p>nnn = Core ID</p> <p>c = L1 colour</p> <p>r = Slice ID</p> <p>mmmm = L2DB ID</p> <p>a = ACP, HWFLUSH or padding</p>

The following table shows the Encodings for ARIDM[12:0].

**Table 8-40: Encodings for ARIDM[12:0]**

Attribute	Value	Issuing capability per ID	Description	Comments
Read ID	0b00nnn00000000	1	Load exclusives, excluding Device Non-Reordering	nnn = Core ID
	0b11ssss0000000	17	Non-Reordering Device reads	sss = Subordinate ID

Attribute	Value	Issuing capability per ID	Description	Comments
	0b10nnncr0ammm	1	READONCE and Main Accelerator Coherency Port (MACP) reads, Atomic read data	nnn = Core ID/ ACP ID c = L1 color or ACP poison  r = Slice ID  mmmm = L2DB ID  a = ACP, HWFLUSH or padding
	0b01nnnrpppppp	1	All other reads	nnn = Core ID r = Slice ID  ppppppp = Internal request ID

nnn is the core number 0b000-0b111 in binary.



These ID and transaction details are provided for information only. Arm strongly recommends that all interconnects and peripherals are designed to support any type and number of transactions on any ID, to ensure compatibility with future products.

For more information about the AXI signals described in this manual, see the [AMBA® AXI Protocol Specification](#).

### 8.7.2.3 MM AXI transactions

The Cortex®-R82AE processor does not generate any FIXED bursts and a burst does not cross a cache line boundary.

The cache linefill fetch length is always 64 bytes.

The Cortex®-R82AE processor generates only a subset of all possible AXI transactions on the manager interface.

For Write-Back Cacheable transfers, the supported transfers are:

- WRAP 2 256-bit for read transfers (linefills).
- INCR 2 256-bit for write transfers (evictions).
- INCR 2 256-bit for read transfers (linefills).
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, 128-bit, and 256-bit for write transfers.

For Normal Non-cacheable or Device transactions:

- INCR 2 256-bit read transfers.

- INCR 2 256-bit write transfers.
- WRAP 2 256-bit read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, 128-bit, and 256-bit read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, 128-bit, and 256-bit write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit exclusive read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit exclusive write transfers.

The following points apply to AXI transactions:

- WRAP bursts are only 256-bit size.
- INCR burst, more than one transfer, are only 256-bit size.
- No transaction is marked as FIXED.
- Write transfers with none, some, or all byte strobes LOW can occur.

#### 8.7.2.4 Support for memory types

The Cortex®-R82AE processor simplifies the coherency logic by downgrading some memory types.

Normal memory that is marked as both Inner Write-Back Cacheable and Outer Write-Back Cacheable is cached in the core data caches and the L2 cache.

All other Normal memory types are treated as Non-cacheable and are sent on the MM port as Normal Non-cacheable.

#### 8.7.2.5 Write response

The AXI manager always accepts write responses without delay by holding BREADY HIGH.

#### 8.7.2.6 AXI4 compatibility mode

The Cortex®-R82AE processor implements an AXI4 compatibility mode that enables you to use the Cortex®-R82AE processor in a standalone environment where the AMBA® AXI5 interface is not required.

To enable this mode, you must ensure that the BROADCASTATOMICM signal is LOW.

Because the Cortex®-R82AE processor is always configured to include RAM protection, it may be necessary to prevent poison from being propagated on the *Main Manager* (MM) interface. This can be achieved by tying CFGMMPOISON to 0 during the integration of the Cortex®-R82AE processor into your system.



### 8.7.2.7 MM AXI privilege information

The *Main Manager* (MM) interface provides information to indicate whether the request is Privileged or Unprivileged on the ARPROTM[0] and AWPROTM[0] signals.

Where a request cannot be merged (Loads and Stores to Device memory, or Non-cacheable Store Exclusives) the ARPROTM[0] and AWPROTM[0] reflect the privilege state of the requestor. Where requests might have been merged, including all Non-cacheable and cacheable loads and stores, the ARPROTM[0] and AWPROTM[0] indicate that the request is privileged.

The MM interface provides information about the Secure or Non-secure access on the ARPROTM[1] and AWPROTM[1] signals. The values of 0 indicates the access is Secure and the value of 1 indicates the access is Non-secure.

The MM interface indicates whether a request is for a data or instruction fetch via the ARPROTM[2] and AWPROTM[2] signals.

## 8.8 LLRAM manager interface

The *Low-latency RAM* (LLRAM) port provides deterministic, low-latency access to external memory shared between cores within the cluster. The Cortex®-R82AE processor has an optional LLRAM manager interface that is shared among the cores within the cluster.

The LLRAM manager interface is a 256-bit AMBA® 5 AXI manager that can be connected to either an AMBA® 4 AXI or an AMBA® 5 AXI subordinate interface.

The LLRAM port does not implement any signals that are not specified in AXI5.

The LLRAM port implements the following signals that are specified in AXI5 but not in AXI4:

- Signal integrity protection signals. These signals are intended to provide point-to-point protection between the Cortex®-R82AE processor cluster and the interconnect and are present bus protection = 1.
- Atomic operation signal, AWATOPL. This signal is used to generate atomic transactions when CFGLLRAMSHARED = 1 and BROADCASTATOMICL = 1.
- Poison signaling

The LLRAM port is expected to have better real-time characteristics compared to the *Main Manager* (MM) port. Because the LLRAM port is shared among the cluster cores, it is expected to have worse real-time characteristics compared to *Tightly Coupled Memories* (TCMs) of individual cores.

To guarantee the deterministic, low-latency characteristics of the LLRAM port, you need to reserve certain buffers in the Cortex®-R82AE processor. For more information, see [8.15 Real-time considerations](#) on page 203.

The LLRAM interface supports accesses to peripherals and also connecting to an interconnect. However, it is not optimized for such accesses. The LLRAM port is mainly used for:

- Code or read/write data shared among cores within the cluster.
- Data sharing between cores within the cluster (producer-consumer).
- Data sharing between cores within the cluster and external agents such as DMA through the *LLRAM Accelerator Coherency Port* (LLRAM ACP, implemented by the *ACE-Lite Subordinate* (ACELS) port).

Accesses to the LLRAM port can only be cached in the L1 data caches and L1 instruction caches as determined by memory type and attributes. The Cortex®-R82AE processor L1 data caches support only Write-Through caching for LLRAM addresses. LLRAM addresses that are marked as Write-Back cacheable are treated as Write-Through.

Accesses to the LLRAM port cannot be cached in the L2 cache. The LLRAM port supports downstream System caches and propagates Cacheable attributes downstream.

LLRAM configuration parameter controls whether the LLRAM interface is implemented or not. If the system does not implement the LLRAM interface ( $LLRAM = 0$ ), the Cortex®-R82AE processor does not include the LLRAM region, port, and coherency logic. All related AXI signals, CFGLLRAMIMP, CFGLLRAMEN, and CFGLLRAMBASEADDR pins are rendered out by the configuration script.

If the system implements the LLRAM interface ( $LLRAM = 1$ ), the Cortex®-R82AE processor includes the LLRAM region, port, and coherency logic. The LLRAM interface can be enabled or disabled by the CFGLLRAMIMP pin and its behavior can be further defined by the CFGLLRAMEN pin. If the LLRAM interface is implemented, the LLRAM region has a fixed size of 256MB.

**Note**

If the LLRAM is not implemented ( $LLRAM = 0$ ) or it is implemented but disabled ( $LLRAM = 1$  and CFGLLRAMIMP tied LOW), associated *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs are not needed to be integrated. See *Arm® Cortex®-R82AE Configuration and Integration Manual* for more information.

---

The LLRAM interface has a size-aligned base address that is set by the configuration signal CFGLLRAMBASEADDR.

The Cortex®-R82AE processor includes hardware coherency logic for addresses in the LLRAM address range so that software does not need to maintain cache coherency for the shared data. The Cortex®-R82AE processor coherency hardware automatically updates the contents of L1 data caches within the cluster to ensure all cores within the cluster have the same coherent view of memory (full coherency).

The coherency hardware also provides coherency with non-cached external agents accessing the LLRAM port through the LLRAM ACP subordinate interface implemented by the ACELS port. The coherency hardware automatically updates the contents of L1 data caches within the cluster but is not able to update the content of managers connected to the LLRAM ACP (I/O coherency).

The LLRAM port is accessible by external agents through the LLRAM ACP subordinate interface. Although it is possible to use an interconnect, this removes the need to add an interconnect between the LLRAM port and the SRAM controller in systems that connect the LLRAM port

directly to an SRAM controller. The LLRAM ACP shares the same physical port, ACELS, as the TCM subordinate port.

If the LLRAM is implemented and not enabled, data accesses to the LLRAM region generate a synchronous External abort.

The Cortex®-R82AE processor LLRAM manager interface supports atomic instructions. The cluster includes logic to perform atomic operations. Whether atomic transactions are generated on the LLRAM port depends on the memory Shareability attributes and the value of CFGLLRAMSHARED and BROADCASTATOMICL signals. This enables you to design systems where the access to memory sub-system is either exclusive to Cortex®-R82AE processor LLRAM port or shared with other manager ports in the system.

In systems where the Cortex®-R82AE processor LLRAM port is the only manager port accessing its memory sub-system components (CFGLLRAMSHARED tied LOW):

- The LLRAM addresses are marked as Non-shareable, Inner Shareable, or Outer Shareable and can be cached in the L1 caches.
- All exclusives and atomic transactions are handled within the cluster.
- No exclusives or atomic transactions are generated on the LLRAM port.

In systems where the Cortex®-R82AE processor LLRAM port is just one of the manager ports into an interconnect and access to the memory sub-system components is shared (CFGLLRAMSHARED tied HIGH):

- The LLRAM addresses that are marked as Outer Shareable cannot be cached in the L1 caches.
- The LLRAM addresses that are marked as Non-shareable or Inner Shareable can be cached in the L1 caches.
- Exclusives transactions can be generated on the LLRAM port.
- Atomic transactions can be generated on the LLRAM port if the BROADCASTATOMICL is HIGH.



Although the LLRAM region can be accessed by EL1 *Virtual Memory System Architecture* (VMSA) contexts, page tables are not allowed to be stored in the LLRAM, and must be stored in memory connected to the MM port instead. If the operating system you are running cannot guarantee that page tables are not placed in the LLRAM region, then you must ensure that the LLRAM region is either disabled or that the operating system does not use the LLRAM region at all. For example, in Linux you can use the *Device Tree* (DT) to specify that the address space occupied by the LLRAM region is reserved memory.

---

## 8.8.1 LLRAM features

The *Low-latency RAM* (LLRAM) manager interface is a 256-bit AMBA® 5 AXI manager. The following table shows LLRAM AXI properties the Cortex®-R82AE processor supports or requires the cluster interconnect and system to support.

**Table 8-41: LLRAM features**

AXI property	Supported by the Cortex®-R82AE processor LLRAM	Interconnect support required
Multi_Copy_Atomicity	Yes	Yes
Ordered_Write_Observation	Yes	Yes
Atomic_Transactions	No  <b>Note:</b> The Cortex®-R82AE processor supports atomic transactions internally on the LLRAM but atomic transactions do not appear on the LLRAM port. For more information, see <a href="#">8.13 Exclusives and atomics support</a> on page 199.	No
Poison	Yes	Yes
Check_Type	No if bus protection is not included (BUS_PROTECTION 0).  Odd_Parity_Byte_All if bus protection is included.	Yes
QoS_Accept	No	No
Trace_Signals	No	No
Loopback_Signals	No	No
Wakeup_Signals	Yes	Yes
Untranslated_Transactions	No	No
NSAccess_Identifiers	No	No
Max_Transaction_Bytes	Yes (64 bytes)	No

## 8.8.2 LLRAM attributes

The following table lists the read and write issuing capabilities for an eight-core Cortex®-R82AE processor.

**Table 8-42: LLRAM attributes**

Attribute	Value	Comments
Write issuing capability	8	The maximum number of writes is 8.  This value can be used by system components to size buffers when bridging to other interface protocols, for example PCIe. Normal Non-cacheable transactions can be removed from this limit by setting the control bit in the IMP_CLUSTERACTLR_EL1.
Read issuing capability	8	The maximum number of reads is 8.
Combined issuing capability	8	The combined issuing capability is 8.
Exclusive thread capability	Number of cores	Each hardware thread can have 1 exclusive access sequence in progress.
Write ID capability	8	The maximum write ID capability is 8.  Only Device memory types with nGnRnE or nGnRE can have more than one outstanding transaction with the same AXI ID. All other memory types use a unique AXI ID for every outstanding transaction.
Write ID width	8	The ID encodes the source of the memory transaction. See the Encodings for AWIDL[7:0] table.
Read ID capability	8	The maximum read ID capability is 8.
Read ID width	8	The ID encodes the source of the memory transaction. See the Encodings for ARIDL[7:0] table.



The issuing capability described here is the maximum possible for the whole cluster. This can be used to size interconnect capabilities if you want to achieve the maximum performance available. However, this maximum may not be reached depending on the Cortex®-R82AE processor configuration and characteristics of your system.

**Table 8-43: Encodings for AWIDL[7:0] and ARIDL[7:0]**

Attribute	Value	Comments
Write ID	0bnnnnmrrr	nnnn is the core number 0b0000-0b0111 in binary. If the nnnn is equal to the number of cores then it is for ACE-Lite Subordinate (ACELS) interface.
		m is 1 for read or write associated with atomics or exclusives. Otherwise m is 0.
		rrr is the internal buffer ID.
Read ID	0bnnnnmrrr	nnnn is the core number 0b0000-0b0111 in binary. If the nnnn is larger or equal to the number of cores then it is for ACELS interface.

Attribute	Value	Comments
		<i>m</i> is 1 for read or write associated with atomics or exclusives and <i>LLRAM Accelerator Coherency Port</i> (LLRAM ACP) accesses. Otherwise <i>m</i> is 0.
		<i>rrr</i> is the internal buffer ID.



Note

These ID and transaction details are provided for information only. Arm strongly recommends that all interconnects and peripherals are designed to support any type and number of transactions on any ID to ensure compatibility with future products.

For more information about the AXI signals described in this manual, see the [AMBA® AXI Protocol Specification](#).

### 8.8.3 LLRAM transactions

The Cortex®-R82AE processor does not generate bursts which cross a cache line boundary.

The cache linefill fetch length is always 64 bytes.

The Cortex®-R82AE processor generates only a subset of all possible AXI transactions on the LLRAM interface.

The following points apply to AXI transactions that are generated by the core:

- Write transfers with none, or some byte strobes LOW can occur.
- Exclusive operations to LLRAM addresses that are marked as Outer Shareable generate exclusive transactions on the port only if CFGLLRAMSHARED is HIGH. Otherwise, they are executed internally.
- Exclusive operations to LLRAM addresses that are not marked as Outer Shareable are handled within the cluster and do not generate exclusive transactions on the LLRAM port.
- Atomic operations to LLRAM addresses that are marked as Outer Shareable generate atomic transactions on the port only if BROADCASTATOMICL and CFGLLRAMSHARED are HIGH. Otherwise, they are executed internally and do not generate atomic transactions (except when BROADCASTATOMICL is LOW and CFGLLRAMSHARED is HIGH, Outer Shareable atomics return SLVERR on the LLRAM port).
- Atomic operations to LLRAM addresses that are not marked as Outer Shareable are executed within the cluster and do not generate atomic transactions on the LLRAM port
- For cacheable memory, D-side accesses, the following accesses are possible:
  - Read transfers:
    - WRAP, 2 beats, 256-bit
  - Write transfers:
    - INCR, 1 beat, 256-bit, address aligned to 256-bits
    - INCR, 1 or 2 beats, 256-bit, address aligned to 512-bits

- For non-cacheable or device memory, the following accesses are possible:
  - Read transfers:
    - INCR, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
  - Write transfers:
    - INCR, 1 beat, 256-bit, address aligned to 256-bits
    - INCR, 1 or 2 beats, 256-bit, address aligned to 512-bits
- For exclusives, the following accesses are possible:
  - Read exclusive transfers:
    - INCR, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bits
  - Write exclusive transfers:
    - INCR, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
- For atomics, the following accesses are possible:
  - Write atomic transfers:
    - 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, 128-bit, or 256-bit

The following points apply to AXI transactions that are generated by the LLRAM ACP:

- Non-modifiable reads with zero length are not modified. The request on the LLRAM port is the same as the initial request received via the ACE-Lite Subordinate (ACELS) port.
- Reads and Writes to Normal memory that are larger than 512 bits, are split into two or more 512-bit transactions.
- Write transfers with none, or some or all byte strobes LOW can occur.
- For modifiable transfers, the following accesses are possible:
  - Read transfers:
    - INCR, 1 or 2 beats, 256-bit
  - Read transfers:
    - INCR or FIXED, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
  - Write transfers:
    - INCR, 1 or 2 beats, 256-bit
- Non-modifiable transfers, the following accesses are possible:
  - Read transfers:
    - INCR or FIXED, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
  - Write transfers:
    - INCR or FIXED, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
- For exclusives, the following accesses are possible:
  - Read transfers:
    - INCR or FIXED, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit

- Write transfers:
  - INCR or FIXED, 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, or 128-bit
- For atomics, the following accesses are possible:
  - 1 beat, 8-bit, 16-bit, 32-bit, 64-bit, 128-bit or 256-bit

## 8.8.4 Support for memory types

The Cortex®-R82AE processor simplifies the coherency logic by downgrading some memory types.

The *Low-latency RAM* (LLRAM) port supports only Write-Through caching. LLRAM addresses that are marked as Write-Back cacheable are treated as Write-Through.

Accesses to the LLRAM port can only be cached in the L1 data caches and L1 instruction caches as determined by memory type and attributes. Accesses to the LLRAM port cannot be cached in the L2 cache.

Only the following memory types can be cached in the L1 data caches:

- Normal memory that is marked as both Inner Write-Through Cacheable and Outer Write-Through Cacheable.
- Normal memory that is marked as both Inner Write-Through Cacheable and Outer Write-Back Cacheable which is treated as Inner and Outer Write-Through.
- Normal memory that is marked as both Inner Write-Back Cacheable and Outer Write-Back Cacheable which is treated as Inner and Outer Write-Through.
- Normal memory that is marked as both Inner Write-Back Cacheable and Outer Write-Through Cacheable which is treated as Inner and Outer Write-Through.

All other Normal memory types are treated as Non-cacheable and are sent on the LLRAM port as Normal Non-cacheable.

Device memory is always treated as non-Gathering, non-Reordering, with no Early Write Acknowledgement (nGnRnE).

## 8.8.5 LLRAM write response

The *Low-latency RAM* (LLRAM) manager always accepts write responses without delay by holding BREADYL HIGH.



### 8.8.6 AXI4 compatibility mode

The Cortex®-R82AE processor implements an AXI4 compatibility mode that enables you to use the Cortex®-R82AE processor in a standalone environment where the AMBA® AXI5 interface is not required.

The *Low-latency RAM* (LLRAM) manager interface performs all atomics within the cluster at the shared level, rather than in the L1 memory system or external memory.

To enable AXI4 compatibility mode, you must ensure that the CFGLLRAMSHARED and RPOISONL signals are LOW.

While the LLRAM port also includes the WPOISONL output signal, this will never be driven HIGH by the Cortex®-R82AE processor and can be safely left unconnected.

### 8.8.7 LLRAM privilege information

The *Low-latency RAM* (LLRAM) manager interface provides information to indicate whether the request is Privileged or Unprivileged on the ARPROTL[0] and AWPROTL[0] signals.

Where a request cannot be merged (Loads and Stores to Device memory, or Non-cacheable Store Exclusives) the ARPROTL[0] and AWPROTL[0] reflect the privilege state of the requestor. Where requests might have been merged, including all Non-cacheable and cacheable loads and stores, the ARPROTL[0] and AWPROTL[0] indicate that the request is privileged.

The LLRAM interface provides information about the Secure or Non-secure access on the ARPROTL[1] and AWPROTL[1] signals. The values of 0 indicates the access is Secure and the value of 1 indicates the access is Non-secure.

The LLRAM interface indicates whether a request is for a data or instruction fetch via the ARPROTL[2] and AWPROTL[2] signals.

## 8.9 MACP subordinate interface

The *Main Accelerator Coherency Port* (MACP) is a 128-bit subordinate interface that conforms to a subset of the ACE5-Lite specification. MACP is a single port attached to the shared L2 and therefore can access data that is shared between all cores in the Cortex®-R82AE processor.

The MACP subordinate interface allows external agents to access memory through the *Main Manager* (MM) interface of the Cortex®-R82AE processor. The MACP subordinate interface provides I/O coherency for external agents with the Cortex®-R82AE processor L1 data and L2 caches (even if the L2 cache size parameter, `L2_CACHE_SIZE` is configured 0).

The `AXCACHE` values of transactions performed via the MACP interface control whether they look-up in the caches. Transactions that are marked as Device, Non-cacheable, or write-through (which is downgraded to Non-cacheable) do not look-up in the cache.

The MACP is optimized for cache line length accesses.

To maintain cache coherency, accesses are checked in all cached locations in the cluster. That is, the L1 data caches in each core and the L2 cache. L1 instruction caches are not checked for coherency because they should be coherent with the external memory.

The MACP supports stash requests from external agents. All stashing requests target the L2 cache and are always cacheline-sized.

### 8.9.1 MACP features

The Cortex®-R82AE processor *Main Accelerator Coherency Port* (MACP) supports the following features.

**Table 8-44: MACP features for the Cortex®-R82AE processor**

MACP property	Supported by the Cortex®-R82AE processor
Port_Type	Accelerator
Continuous_Cache_Line_Read_Data	Yes
Multi_Copy_Atomicity	Yes
Ordered_Write_Observation	No
WriteEvict_Transaction	No
DVM_v8	No
Atomic_Transactions	Yes
DVM_v8.1	No
Cache_Stash_Transactions	Yes
DeAllocation_Transactions	No
Persistent_CMO	No
Poison	No
Check_Type	Yes, if bus protection is enabled
Check_Type	No
QoS_Accept	No
Trace_Signals	No
Loopback_Signals	No
Wakeup_Signals	Yes
Untranslated_Transactions	No
NSAccess_Identifiers	No

## 8.9.2 MACP attributes

For optimum performance, use the following guidelines for the *Main Accelerator Coherency Port* (MACP) transactions.

WriteUniquePtl transactions always incur a read-modify write sequence.

L2 resources are shared between the MACP and the cores. Therefore, heavy traffic on the MACP might, in some cases, reduce the performance of the cores.

Read transactions cannot allocate to the L1 cache, but use the Write-back Read-Allocate bits of the memory type (ARCCACHEA) to decide whether to allocate to the L2 cache.

Write transactions cannot allocate to the L1 cache, but use the Write-back Write-Allocate bits of the memory type (AWCCACHEA) to decide whether to allocate to the L2 cache. Compared to WriteUniqueFull, a WriteUniqueFullStash that targets allocation to the L2 cache is optimized to reduce the latency of a core read request that occurs shortly after the write request.

The following table describes the MACP attributes.

**Table 8-45: MACP attributes**

Attribute	Value	Description
Write acceptance capability	5	The MACP can accept up to five write transactions.
Read acceptance capability	5	The MACP can accept up to five read transactions.
Combined acceptance capability	6	The MACP can accept up to six transactions with: <ul style="list-style-type: none"> <li>One read transaction and one write transaction</li> <li>Up to four read transactions or write transactions</li> </ul>
Write ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.
Read ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.

## 8.9.3 MACP transaction types

The *Main Accelerator Coherency Port* (MACP) supports read and write transaction types with the same transfer size and length combinations.

The following table describes the MACP read and write transactions.



Note

- x in the signal names is used to refer to both read and write signals. For example, AxLENA refers to both ARLENA and AWLENA signals.
- For all the write transactions,WSTRBA, any combination of bytes, including no bytes, are valid.

**Table 8-46: Read and write transactions**

Transaction	AxLENA	AxSIZEA	AxADDRA
1-byte INCR	0 (one beat)	0 (single byte)	-
2-byte INCR	0 (one beat)	1 (two bytes)	0b0 (Address aligned to 2-byte boundary)
4-byte INCR	0 (one beat)	2 (four bytes)	0b00 (Address aligned to 4-byte boundary)
8-byte INCR	0 (one beat)	3 (eight bytes)	0b000 (Address aligned to 8-byte boundary)
16-byte INCR	0 (one beat)	4 (16 bytes)	0b0000 (Address aligned to 16-byte boundary)
32-byte INCR	1 (two beats)	4 (16 bytes)	0b00000 (Address aligned to 32-byte boundary)
64-byte INCR	3 (four beats)	4 (16 bytes)	0b000000 (Address aligned to 64-byte boundary)



Note

The AMBA 5 ACE-Lite transaction types WriteUniqueFull and WriteUniquePtl were known in AMBA 4 ACE-Lite as WriteLineUnique and WriteUnique, respectively.

The following table lists the transaction types that are supported by the MACP:

**Table 8-47: MACP supported transaction types**

Transaction group	Transaction type
Read	ReadOnce
	ReadNoSnoop
Write	WriteUniquePtl
	WriteUniqueFull
	WriteUniqueFullStash
	WriteUniquePtlStash
	WriteNoSnoop
	StashOnceUnique
	StashOnceShared
Cache maintenance	CleanShared
	CleanInvalid
	MakeInvalid

Transaction group	Transaction type
Atomics	AtomicStore*
	AtomicLoad*
	AtomicSwap
	AtomicCompare

### 8.9.3.1 MACP transaction restrictions

The *Main Accelerator Coherency Port* (MACP) conforms to a subset of the ACE5-Lite specification.

The ACE5-Lite is described in the [AMBA® AXI Protocol Specification](#).

All transactions can be Secure or Non-secure.

All requests can specify Outer Shareable and Non-shareable using the AWDOMAINA and ARDOMAINA signals.

ARQOS and AWQOS signals are not present.

The Cortex®-R82AE processor has the following additional restrictions on MACP. The requests that do not meet these restrictions generate a SLVERR response on RRESPA or BRESPA:

- Transactions with a length of more than one transfer are not supported when AxCACHEA[1] is 0.
- Exclusive accesses are not supported. ARLOCK and AWLOCK signals are not present.
- Barriers are not supported. The BRESPA response for any write transaction indicates global observability for the transaction.
- ARSIZEA and AWSIZEA signals are present. Only combinations of transaction address, burst length and burst size resulting in the following will be supported:
  - The total amount of data transferred is a power of 2, from one byte to a maximum of 64 bytes (one Cortex®-R82AE processor cache line).
  - The burst address is aligned to the total amount of data transferred.
- The values of ARLENA and AWLENA are restricted to:
 

<b>0</b>	One beat
<b>1</b>	Two beats
<b>3</b>	Four beats
- ARBURST and AWBURST signals are present. Only a value of 0b01 (INCR) is supported.
- Only the following Atomic sizes and lengths are supported:
  - For AtomicStore\*, AtomicLoad\*, and AtomicSwap: 1 byte, 2 bytes, 4 bytes, and 8 bytes
  - For AtomicCompare: 2 bytes, 4 bytes, 8 bytes, 16 bytes, and 32 bytes

## 8.10 ACELS interface

The *ACE-Lite Subordinate* (ACELS) interface is a 128-bit ACE5-Lite subordinate interface that is shared between all cores in the Cortex®-R82AE processor. It provides external access to the *Tightly Coupled Memories* (TCMs) and the *Low-latency RAM* (LLRAM) port.

The Cortex®-R82AE processor provides optional AMBA interface parity checks on the ACELS interface.

The ACELS interface is used for two purposes:

- As a TCM subordinate enabling agents outside the cluster to access TCMs within the cores. The TCM subordinate also enables the cores within the Cortex®-R82AE processor to access the TCMs of other cores through an interconnect loopback.
- As an LLRAM *Accelerator Coherency Port* (LLRAM ACP) enabling coherent external access to the LLRAM port.

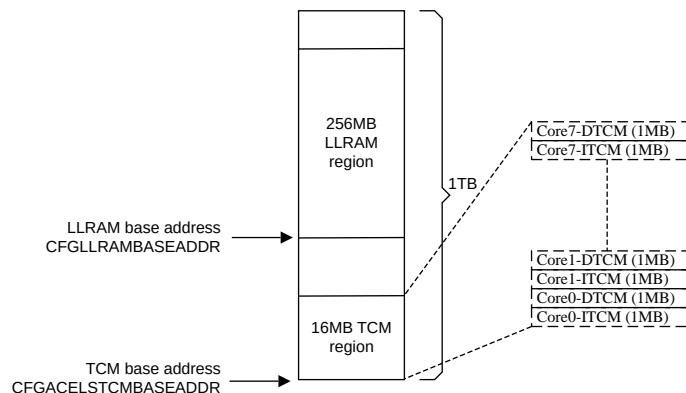
Both of these functions are provided by the same physical port, ACELS, that responds to two different ranges of address, one for the TCM subordinate and one for the LLRAM ACP. However, they are described as separate concepts in this chapter.

The Cortex®-R82AE processor TCM subordinate and LLRAM ACP address regions must not overlap. The Cortex®-R82AE processor ACELS interface generates SLVERR error response to access requests that fall within both the TCMs and the LLRAM ACP addresses.

The ACELS interface uses base addresses for routing the access to the 16MB TCM region and 256MB LLRAM ACP region:

- The 16MB TCM region is divided into eight 2MB blocks, one for each core. TCMs (ITCM and DTCM) within a core are mapped into two 1MB regions.
- The LLRAM ACP address region is the same as the LLRAM address region visible to the cores within the Cortex®-R82AE processor.

The following figure shows how each TCM and the LLRAM ACP are mapped into the ACELS interface address space.

**Figure 8-5: ACELS memory map**

The ACELS memory map is unchanged irrespective of whether the Cortex®-R82AE processor is configured to operate in Split-mode, Lock-mode, or Hybrid-mode. However, when operating in Lock-mode, the TCMs must only be accessed by addressing the physical cores. This means that accesses can only be made to even-numbered cores in the TCM region and accesses to the redundant cores (which are odd-numbered) will return a decode error without forwarding the request to the TCMs.

The ACELS port is typically connected to an interconnect, through which various system agents can access the TCMs and LLRAM port.

Even though the TCM subordinate and LLRAM ACP share the ACELS port, they operate largely independently. The ACELS port supports out-of-order completion between accesses to each core's TCM subordinates and accesses to the LLRAM port. The ACELS transactions with different ACE IDs are able to complete out-of-order.

For any request that is targeting the TCM subordinate and LLRAM ACP, the total amount of data transferred is a power of 2 and can be greater than 64 bytes that is one Cortex®-R82AE processor cache line.

The Cortex®-R82AE processor ACELS port does not create ordering dependencies between the ACELS reads and writes, or between the ACELS reads with different IDs, or between the ACELS writes with different IDs.

The Cortex®-R82AE processor ACELS AXI ID signals are 8 to 24 bits wide and configured with the `ACELS_ID_WIDTH` parameter. In order for an AXI or ACE-Lite manager with an ACE ID width larger than the Cortex®-R82AE processor ACELS AXI ID width to access the ACELS port, that manager must be connected through logic that compresses the AXI ID signals. The Cortex®-R82AE processor does not provide such logic.

The ACELS port contains enough buffering to support 128-bit per cycle sustained transfers to/from TCM or LLRAM port memory with no wait state. However, the ACELS port might be unable

to immediately accept a transaction request and might instead apply back-pressure on the port when many transactions to TCM or LLRAM port memory with wait states are outstanding.

The ACELS port includes ARLOCK and AWLOCK pins, but only supports single beat exclusives to the LLRAM ACP. Exclusives targeting the LLRAM ACP with AXLENS not set to 0 are not supported and will return a subordinate error. Furthermore, exclusives are not supported to the TCM subordinate and all exclusive requests targeting the TCM subordinates will not return an EXOKAY response and will therefore fail the exclusive access.

The ACELS port includes the AWATOP pins to ease integration with an AXI or ACE manager that includes atomic support. The ACELS port only supports atomics for the LLRAM ACP. Any atomic request targeting the TCM subordinate will return a SLVERR response.

For atomics with a load component (AtomicLoad, AtomicStore and AtomicCompare), the read response and write response are not guaranteed to be consistent. For example, the read response might return OKAY if the read completed successfully while the write might return an error response if the write component fails. It is recommended the manager connected to the ACELS port consumes both the read and write response in order to determine if the atomic has completed successfully.

### 8.10.1 ACELS features

The Cortex®-R82AE processor *ACE-Lite Subordinate* (ACELS) interface supports the following features.

**Table 8-48: ACELS features for the Cortex®-R82AE processor**

ACELS property	Supported by the Cortex®-R82AE processor
Port_Type	Accelerator
Continuous_Cache_Line_Read_Data	Yes
Multi_Copy_Atomicity	Yes
Ordered_Write_Observation	No
WriteEvict_Transaction	No
DVM_v8	No
Atomic_Transactions	Yes <b>Note:</b> Atomics are supported for LLRAM ACP but not for the TCM subordinate. Atomic requests targeting TCM subordinate will return a SLVERR response.
DVM_v8.1	No
Cache_Stash_Transactions	No
DeAllocation_Transactions	No
Persistent_CMO	No
Poison	No
Check_Type	Yes, if bus protection is enabled.
Check_Type	No



ACELS property	Supported by the Cortex®-R82AE processor
QoS_Accept	No
Trace_Signals	No
Loopback_Signals	No
Wakeup_Signals	Yes
Untranslated_Transactions	No
NSAccess_Identifiers	No

### 8.10.2 ACELS attributes

For optimum performance, use the following guidelines for *ACE-Lite Subordinate* (ACELS) interface transactions.

WriteUniquePtl transactions are sent out on the ACE-Lite bus.

Some L1 and *LLRAM Coherency Unit* (LCU) memory system resources are shared between the ACELS interface and the cores. Therefore, heavy traffic on the ACELS interface might, in some cases, reduce the performance of the cores.

The following table describes the ACELS attributes where NUM\_CORES is the number of logical cores from 1 to 8.

**Table 8-49: ACELS attributes**

Attribute	Value	Description
Write acceptance capability	$(8 * \text{NUM\_CORES}) + 10$	The write acceptance capability is dependent on the number of cores. For example, an MP4 configuration has a theoretical acceptance capability of 42 write transactions.
Read acceptance capability	$(7 * \text{NUM\_CORES}) + 10$	The read acceptance capability is dependent on the number of cores. For example, an MP4 configuration has a theoretical acceptance capability of 38 read transactions.
Combined acceptance capability	Write acceptance capability + Read acceptance capability - $(4 * \text{NUM\_CORES})$	The combined acceptance capability is dependent on the number of cores. For example, an MP4 configuration has a theoretical acceptance capability of 44 transactions.
Write ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.
Read ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.

### 8.10.3 ACELS transaction types

The *ACE-Lite Subordinate* (ACELS) interface conforms to the ACE5-Lite specification.

The Cortex®-R82AE processor ACELS interface supports the majority of ACE5-Lite burst types and lengths. See [8.10.3.1 ACELS transaction restrictions](#) on page 190 for the restrictions that apply to the ACELS interface.

For more information on the ACE5-Lite, see the [AMBA® AXI Protocol Specification](#).

The following table lists the transaction types that are supported by the ACELS.

**Table 8-50: ACELS supported transaction types**

Transaction group	Transaction type
Read	ReadOnce
	ReadNoSnoop
Write	WriteUniquePtl
	WriteUniqueFull
	WriteNoSnoop
Atomics <b>Note:</b> Atomics are supported for LLRAM ACP but not for the TCM subordinate. Atomic requests targeting TCM subordinate will return a SLVERR response.	AtomicStore
	AtomicLoad
	AtomicSwap
	AtomicCompare

#### 8.10.3.1 ACELS transaction restrictions

The following transactions cause SLVERR or DECERR error on the *ACE-Lite Subordinate* (ACELS) interface.

The following cases generate a SLVERR response on RRESPS or BRESPS:

- Non-modifiable bursts (ARCACHES[1] or AWCACHES[1] is set to 0) when ARLENS > 0 or AWLENS > 0.
- ARSNOOPS is non-zero, or AWSNOOPS[3:1] is non-zero.
- Non-secure access to the TCM subordinate when ARPROTS[1] or AWPROTS[1] is set to 1.
- Atomic requests to the TCM subordinate.
- Non-single-beat exclusive requests to the LLRAM ACP (ARLENS > 0)
- IMP\_CLUSTERACELSCTLR\_EL1[x] is set to 0, where x is the (core number \* 2) that the accessed TCM belongs to.
- IMP\_CLUSTERACELSCTLR\_EL1[x] is set to 0 and ARPROTS[0] or AWPROTS[0] is set to 0, where x is the (core number \* 2) + 1 that the accessed TCM belongs to.
- TCM subordinate access to a powered off core.

- Double bit error on a read to the *Tightly Coupled Memories* (TCMs).
- SLVERR response from the *Low-latency RAM* (LLRAM) interface as a response to an access from the LLRAM ACP.

The following cases generate a DECERR response on RRESPS or BRESPS:

- Access to the region of ACELS memory map if the address falls outside both the LLRAM and TCM regions.
- Access to the region of ACELS memory map if the address falls into both the LLRAM and TCM regions.
- Access to the gap in ACELS memory map between TCMs.
- DECERR response from the LLRAM interface as a response to an access from the LLRAM ACP.
- Access to the TCM region of a non-existent core.
- Access to the TCM region of a redundant core when operating in Lock-mode.

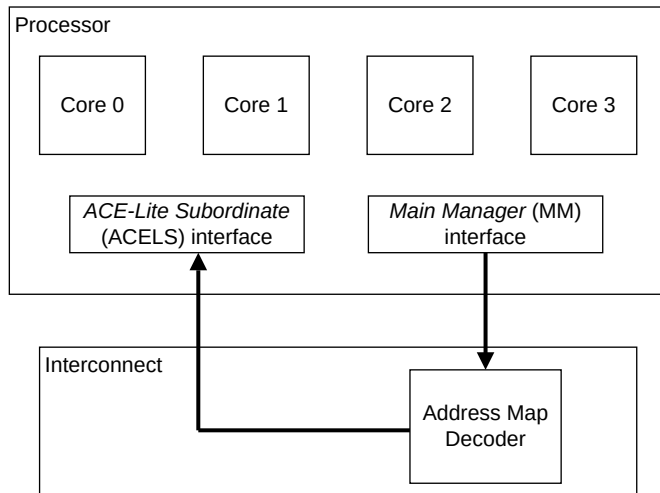
The following cases generate an OK response on RRESPS or BRESPS:

- An exclusive (locked) read access to the TCM region, except where a SLVERR or DECERR occurs.
- An exclusive (locked) write access to the TCM region, except where a SLVERR or DECERR occurs.

#### 8.10.4 TCM subordinate

The Cortex®-R82AE processor TCM subordinate enables agents outside the cluster to access all the TCMs within the Cortex®-R82AE cluster. It also enables any core within the Cortex®-R82AE processor to access all the TCMs within the cluster, except its own, via an interconnect loopback, that is assuming the *ACE-Lite Subordinate* (ACELS) port is connected to the interconnect and the Cortex®-R82AE processor is able to access the ACELS port through regular *Main Manager* (MM) memory accesses to the address region starting at CFGACELSTCMBASEADDR. The software running on any given core within the Cortex®-R82AE processor shall not access its own TCMs via the TCM subordinate. It shall use the private addresses defined by CFGITCMBASEADDRm or CFGDTCMBASEADDRm to access its own TCMs.

The following figure shows an example of a loopback address mapping for a core access to the ACELS through the interconnect. It is recommended that the Main Manager interface is used for loopback to the TCMs via TCM subordinate, and not the LLRAM, LLPP or SPP interfaces.

**Figure 8-6: Loopback address mapping**

The Cortex®-R82AE processor TCM subordinate is capable of sustaining 128 bits per cycle of:

- Read bandwidth when reading from any number of TCMs with no wait states. This assumes no contention for accessing the TCMs.
- Write bandwidth when writing to any number of TCMs with no wait states. This assumes no contention for accessing the TCMs.

As the TCMs are banked for efficient sharing between the core and the TCM subordinate, the Cortex®-R82AE processor TCM subordinate bandwidth tends towards 128 bits per cycle when both a core and the TCM subordinate access the same TCM with no wait state sequentially.

The Cortex®-R82AE processor TCM subordinate address space is a 16MB region located at a 16MB-aligned base address set by the configuration input signal `CFGACELSTCMBASEADDR[PA_W-1:24]`, providing access to all TCM memories within the processor. The base address set by the configuration input signal `CFGACELSTCMBASEADDR[PA_W-1:24]` must match the address the ACELS port in the system memory map.

The 16MB region is divided into eight 2MB blocks, one for each core. Each 2MB block is subdivided into two 1MB regions. TCMs (ITCM and DTCM) within a core are mapped into two 1MB regions. The lower 1MB is mapped to the ITCM and the upper 1MB to the DTCM. If the size of any TCM is less than the maximum 1MB, the remaining upper part will be inaccessible and return a DECERR response.

The memory map is the same regardless of the number of cores configured, and the sizes and number of TCMs present. Regions associated with cores that are not present generate a DECERR response. If a TCM is accessed outside of its configured range, the TCM subordinate generates a DECERR error response. Such accesses include addresses that map to cores which have not been implemented, addresses which do not map to any TCM, and addresses that map to a TCM but are too high for the implemented size of that TCM.

For each core, access control checks can be enabled for the TCM subordinate transactions by programming `IMP_CLUSTERACELCTRL.TCMACCLVL`. Access control allows either all transactions or only privileged transactions to access the TCM. If a transaction is not permitted, the TCM subordinate generates a `SLVERR` response.

For transaction requests that target cores which have been powered down, the TCM subordinate generates a `SLVERR` error response.

If the Cortex®-R82AE processor TCM subordinate accesses TCMs in a core which is in WFI or WFE low-power state but not in a retention or power down state, then the access proceeds. In this case, the clocks to the core are re-enabled if necessary.

#### 8.10.4.1 Accessing TCMs configured with ECC

When a *Tightly Coupled Memory* (TCM) implements *Error Correcting Code* (ECC), the ECC is generated within the core before writing to the TCM.

If the core detects an error on reads or writes the behavior is:

##### **Writes**

- If a write to TCM requires a read-modify-write, and a correctable error is detected when reading the TCM, the ECC is recalculated.
- If a write to TCM requires a read-modify-write, and a non-correctable error is detected when reading the TCM, a `SLVERR` response is returned.

##### **Reads**

- For a correctable error, the core corrects the data and returns corrected data with `OKAY` response.
- For a non-correctable error, a `SLVERR` response is returned.

#### 8.10.4.2 TCM subordinate attributes

This section describes the capabilities and attributes of the TCM subordinate interface.

The TCM subordinate interface does not support:

- Exclusive transactions, therefore, `AmLOCK` is not used.
- Data and instruction transaction signaling, therefore, `AmPROT[2]` is not used.
- QoS is not supported, therefore, `AmQOS` is not used.
- Multiple address region signaling is not supported, therefore, `AmREGION` is not used.

The following table shows the TCM subordinate interface attributes where `NUM_CORES` is the number of logical cores from 1 to 8.

**Table 8-51: TCM subordinate interface attributes**

Attribute	Value	Comments
Write acceptance capability	NUM_CORES * 8	The maximum number of outstanding write transactions that a subordinate can accept.
Read acceptance capability	NUM_CORES * 7	The maximum number of outstanding read transactions that a subordinate can accept.
Combined acceptance capability	NUM_CORES * 15	The maximum number of outstanding transactions that a subordinate can accept.
Write ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.
Read ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.

### 8.10.5 LLRAM ACP

The *Low-latency RAM Accelerator Coherency Port* (LLRAM ACP) enables agents outside the cluster to access the LLRAM port coherently. The *ACE-Lite Subordinate* (ACELS) interface routes accesses to addresses within the LLRAM ACP address region to the LLRAM ACP. The LLRAM ACP address region is the same as the LLRAM address region visible to the cores within the Cortex®-R82AE processor.

The Cortex®-R82AE processor includes coherency hardware that automatically manages the contents of the L1 data caches within the cluster to ensure all cores within the cluster and uncached agents connected to the LLRAM ACP have a coherent view of LLRAM addresses.

The LLRAM ACP is capable of sustaining 128 bits per cycle of:

- Read bandwidth when reading from the LLRAM. This assumes no contention for accessing the LLRAM.
- Write bandwidth when writing to the LLRAM. This assumes no contention for accessing the LLRAM.

The LLRAM ACP interface provides information to indicate whether the request is Privileged or Unprivileged on the ARPROTL[0] and AWPROTL[0] signals.



Note

- A Cacheable transaction from the Cortex®-R82AE processor or ACELS interface is always indicated as Privileged (ARPROTL[0] = 1 and AWPROTL[0] = 1).
- A Non-cacheable or Device transaction from the ACELS interface has the incoming ARPROTS[0] and AWPROTS[0] values.

The LLRAM ACP provides information about the security attributes of accesses on the ARPROTL[1] and AWPROTL[1] signals. The value of 0 indicates the access is Secure and the value of 1 indicates the access is Non-secure.

The LLRAM ACP interface indicates whether a request is for a data or instruction fetch via the ARPROTL[2] and AWPROTL[2] signals.

### 8.10.5.1 LLRAM ACP attributes

This section describes the capabilities and attributes of the Cortex®-R82AE processor *Low-latency RAM Accelerator Coherency Port* (LLRAM ACP).

The Cortex®-R82AE processor LLRAM ACP does not support:

- QoS is not supported, therefore, AmQOS is not used.
- Multiple address region signaling is not supported, therefore, AmREGION is not used.
- Barriers are not supported. The write response for any write request indicates global observation of that write.

The following table shows the Cortex®-R82AE processor LLRAM ACP attributes.

**Table 8-52: LLRAM ACP attributes**

Attribute	Value	Comments
Write acceptance capability	12	The maximum number of outstanding write transactions that a subordinate can accept.
Read acceptance capability	12	The maximum number of outstanding read transactions that a subordinate can accept.
Combined acceptance capability	14	The maximum number of outstanding read and write transactions that a subordinate can accept.
Write ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.
Read ID width	8 to 24 bits	Unused bits tied to zero if fewer bits required.

## 8.11 Utility bus

The Utility bus provides access to control registers for various system components in the Cortex®-R82AE processor. The Utility bus is implemented as a 64-bit AMBA® 5 AXI subordinate port.

The Utility bus provides memory-mapped access to the following register families:

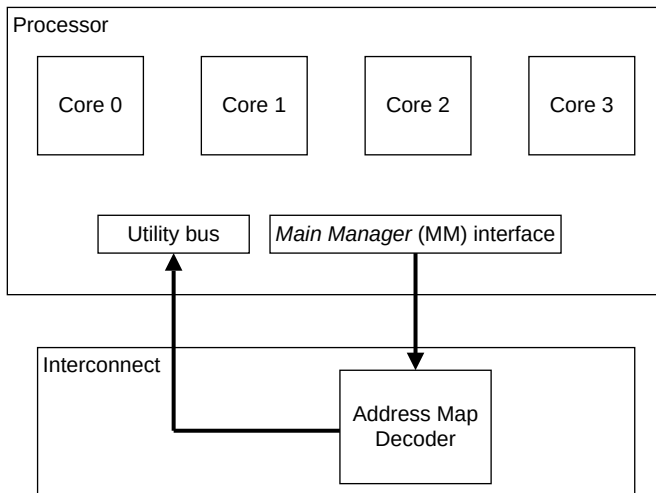
- Per-core and the cluster *Power Policy Units* (PPUs) registers.
- Per-core *Reliability, Availability, and Serviceability* (RAS) registers.
- Per-core and the cluster *Programmable MBIST Controller* (PMC) registers.
- Per-core *Software Built In Self Test Controller* (SBIST) registers.

If your system has a *System Control Processor* (SCP), the Utility bus enables the SCP to manage the power policy and the error handling of the Cortex®-R82AE processor.

If your system does not have an SCP or the SCP is limited in its scope, you can connect the Utility bus to the system interconnect. A core within the Cortex®-R82AE processor, then, can access all the PPU and the RAS registers through the *Main Manager* (MM) port which is connected via a loopback to the Utility bus.

The following figure shows an example of a loopback address mapping for a core access to the Utility bus through the interconnect.

**Figure 8-7: Loopback address mapping**



Note

The Cortex®-R82AE processor supports the loopback address mapping between the following ports:

- The MM port to the Utility bus.
- The *Shared Peripheral Port* (SPP) to the Utility bus.
- The MM port to the *ACE-Lite Subordinate* (ACELS) port.

### 8.11.1 Utility bus accesses

Transactions on the Utility bus comply with a subset of the AXI 5 bus protocol. Accesses must be either 32-bits or 64-bits. Any other sized access generates a SLVERR response from the Utility bus.

You must observe the following requirements when accessing Utility bus:

- Only ReadNoSnoop and WriteNoSnoop transaction types are supported.
- Only 32-bit accesses or 64-bit accesses are supported. Therefore, ARSIZEU or AWSIZEU must be either 0b010 for 32-bit sized accesses, or 0b011 for 64-bit sized accesses. Any other access size generates a SLVERR response from the Utility bus.
- Only single beat bursts are supported. Therefore, ARLENU or AWLENU must be 0b00000000. Any other burst length generates a SLVERR response from the Utility bus.
- All system components control registers only support Secure accesses and data accesses on the Utility bus. Any accesses to these registers with the Non-secure bit set generate a SLVERR response.



- No exclusives supported. The Utility bus treats them as plain accesses and does not abort them.
- No atomics supported.

Arm recommends the following when accessing the Utility bus:

- ARCACHEU or AWCACHEU is either 0b0000 or 0b0001, although other values are accepted and ignored.
- ARBURSTU or AWBURSTU is 0b01, although other values are accepted and ignored.
- ARLOCKU or AWLOCKU is tied LOW, as there is no exclusive monitor present.

The following table describes the Utility bus attributes.

**Table 8-53: Utility bus attributes**

Attribute	Value	Description
Write acceptance capability	1	The Utility bus can accept one write transaction.
Read acceptance capability	1	The Utility bus can accept one read transaction.
Combined acceptance capability	2	The Utility bus can accept up to two transactions.
Write ID width	1 to 24 bits	Unused bits tied to zero if fewer bits required.
Read ID width	1 to 24 bits	Unused bits tied to zero if fewer bits required.

### 8.11.2 Base addresses for system components

Each set of system registers is grouped on separate 64KB page boundaries allowing access control to be enforced by the memory management. An alternative 4kB register spacing can be selected using the `DENSE_CS_ADDR_MAP` parameter.

See [B.1.2.2.3 PPU\\_PWSR, Power Status Register](#) on page 1569 for information on the base addresses for each set of system component registers that the external agents can access using the Utility bus.

## 8.12 Direct access to internal memories

The Cortex®-R82AE processor provides a mechanism to read the internal memories that are used by the L1 and L2 caches and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs and TLB structures through **IMPLEMENTATION DEFINED** System registers.

This functionality enables direct reading of cache RAMs by software and can be useful when investigating issues where the coherency between the data in the cache and data in the system memory is broken.

### 8.12.1 Direct access to L1 memory

The Cortex®-R82AE processor provides a mechanism to read the internal memories that are used by the L1 caches and TLB structures through **IMPLEMENTATION DEFINED** System registers.

The appropriate memory block and location are selected using one of several system instructions. The data is read from read-only registers after performing the appropriate Read Operation system instruction. These operations are available both in EL1 and EL2 but EL1 accesses can be trapped using ACTLR\_EL2.CDBG. In EL0, executing these instructions results in an Undefined Instruction exception.

The following table shows the system registers and system instructions to access L1 memory.

**Table 8-54: System registers and system instructions used to access L1 memory**

Register name	Function	Access	Operation	Register Data
IMP_CDBGDR0_EL1	Cache Debug Data Register 0	Read-only	MRS <Xt>, S3_2_c15_c0_0	Data
IMP_CDBGDR1_EL1	Cache Debug Data Register 1	Read-only	MRS <Xt>, S3_2_c15_c0_1	Data
SYS IMP_CDBGDCT	L1 Data Cache Tag Read Operation	System instruction	SYS S1_2_c15_c2_0, <Xt>	Set/Way
SYS IMP_CDBGICT	L1 Instruction Cache Tag Read Operation	System instruction	SYS S1_2_c15_c2_1, <Xt>	Set/Way
SYS IMP_CDBGTT	TLB Tag Read Operation	System instruction	SYS S1_2_c15_c2_2, <Xt>	Index/Way
SYS IMP_CDBGDCD	L1 Data Cache Data Read Operation	System instruction	SYS S1_2_c15_c4_0, <Xt>	Set/Way/Offset
SYS IMP_CDBGICD	L1 Instruction Cache Data Read Operation	System instruction	SYS S1_2_c15_c4_1, <Xt>	Set/Way/Offset
SYS IMP_CDBGTD	TLB Data Read Operation	System instruction	SYS S1_2_c15_c4_2, <Xt>	Index/Way

Execution of one of the SYS IMP\_CDBGDCT, SYS IMP\_CDBGICT, SYS IMP\_CDBGDCD or SYS IMP\_CDBGICD operations must be followed by a read of IMP\_CDBGDR0\_EL1 register, and if necessary by a subsequent read of IMP\_CDBGDR1\_EL1 register. Similarly, a read from IMP\_CDBGDR0\_EL1 or IMP\_CDBGDR1\_EL1 registers must have been preceded by execution of one of the SYS IMP\_CDBGDCT, SYS IMP\_CDBGICT, SYS IMP\_CDBGDCD or SYS IMP\_CDBGICD operations.

To specify the cache line from which you want to read, use the bit description table in the system register description.

### 8.12.2 Direct access to L2 and LCU memory

The Cortex®-R82AE processor provides a mechanism to read the internal memories that are used by the L2 cache and the *LLRAM Coherency Unit* (LCU) and TLB structures through **IMPLEMENTATION DEFINED** System registers.

The appropriate memory block and location are selected using one of several system instructions. The data is read from read-only registers after performing the appropriate Read Operation system instruction. These operations are available both in EL1 and EL2 but EL1 accesses can be trapped using ACTLR\_EL2.CDBG. In EL0, executing these instructions results in an Undefined Instruction exception.

The following table shows the system registers and system instructions to access L2 and LCU memories.

**Table 8-55: System registers and system instructions used to access L2 and LCU memories**

Register name	Function	Access	Operation	Register Data
IMP_CLUSTERCDBGDR0_EL1	Cluster Cache Debug Data Register 0	Read-only	MRS <Xt>, S3_2_c15_c3_0	Data
SYS IMP_CLUSTERCDBGL2D	L2 Cache Data Read Operation	System instruction	SYS S1_2_c15_c4_3, <Xt>	Set/Way
SYS IMP_CLUSTERCDBGL2DT	L2 Cache Duplicate L1 Tag Read Operation	System instruction	SYS S1_2_c15_c3_3, <Xt>	Set/Way
SYS IMP_CLUSTERCDBGL2T	L2 Cache Tag Read Operation	System instruction	SYS S1_2_c15_c2_3, <Xt>	Index/Way
SYS IMP_CLUSTERCDBGLCUdT	LCU Duplicate L1 Tag Read Operation	System instruction	SYS S1_2_c15_c3_4, <Xt>	Set/Way/Offset

Execution of one of the SYS IMP\_CLUSTERCDBGL2D, SYS IMP\_CLUSTERCDBGL2DT, SYS IMP\_CLUSTERCDBGL2T or SYS IMP\_CLUSTERCDBGLCUdT operations must be followed by a read of IMP\_CLUSTERCDBGDR0\_EL1 register. Similarly, a read from IMP\_CLUSTERCDBGDR0\_EL1 register must have been preceded by execution of one of the SYS IMP\_CLUSTERCDBGL2D, SYS IMP\_CLUSTERCDBGL2DT, SYS IMP\_CLUSTERCDBGL2T or SYS IMP\_CLUSTERCDBGLCUdT operations.

To specify the cache line from which you want to read, use the bit description table in the System register description.

## 8.13 Exclusives and atomics support

The Cortex®-R82AE processor supports load/store exclusive and atomic instructions on some interfaces and not on others.

The Cortex®-R82AE processor does not support exclusives and atomics for the following cases:

- Software running from a core within the Cortex®-R82AE processor executing load/store exclusive or atomic instructions accessing the *Low-latency Peripheral Port* (LLPP) region. A synchronous External abort is taken if software executes an exclusive or atomic targeting the LLPP.
- Software running from a core within the Cortex®-R82AE processor executing load/store exclusive or atomic instructions accessing the *Shared Peripheral Port* (SPP) region. A synchronous External abort is taken if software executes an exclusive or atomic targeting the SPP.
- Incoming atomic or exclusive transactions on the TCM subordinate implemented by the *ACE-Lite Subordinate* (ACELS) interface. A SLVERR response is returned if software executes an atomic request targeting the TCM subordinate. An OK response is returned if software executes an exclusive request targeting the TCM subordinate, failing any exclusive requests.

- Incoming non-single-beat exclusive transactions on the *LLRAM Accelerator Coherency Port* (LLRAM ACP) implemented as ACE-Lite Subordinate (ACELS) interface. A SLVERR response is returned if software executes an exclusive request with ARLENS>0 targeting the LLRAM ACP.
- Incoming cacheable atomic or exclusive transactions on the *Main Accelerator Coherency Port* (MACP). A SLVERR response is returned if software executes a cacheable atomic request targeting the MACP but Non-cacheable atomics are supported. The MACP cannot receive exclusive requests (AxLock is not implemented) and can therefore only return an OK response, failing any exclusive requests.
- Incoming atomic or exclusive transactions on the Utility bus. The Utility bus cannot receive exclusive requests (AxLock is not implemented) and can therefore only return an OK response, failing any exclusive requests. The Utility bus cannot receive atomic requests (AWATOP is not implemented) and therefore cannot receive atomic requests. It is the responsibility of the system to abort any atomics targeting the Utility bus.

You can build systems that do not require support for exclusives or atomics outside the Cortex®-R82AE processor. However, if your system requires support for exclusives outside the Cortex®-R82AE processor, the system must implement a global exclusive access monitor. The global access monitor must signal to the Cortex®-R82AE processor through the EVENTIREQ input when it is cleared.

The following table describes the support for exclusives and atomics for the following cases:

- Software running from a core within the Cortex®-R82AE processor executing load/store exclusive or atomic instructions accessing the *Low-latency RAM* (LLRAM) region.
- Incoming transactions on the *LLRAM Accelerator Coherency Port* (LLRAM ACP) implemented as *ACE-Lite Subordinate* (ACELS) interface.



Note

- LLRAM ACP System Shareable transactions are treated as Outer Shareable.
- X in the following table means that the value can be either HIGH or LOW.

**Table 8-56: Exclusives and atomics support for LLRAM and LLRAM ACP**

Type	Shareability	CFGLLRAMSHARED	BROADCASTATOMICL	Access to LLRAM region	Incoming LLRAM ACP transaction
Exclusives	Non-shareable	X	X	Executed in cluster	
	Inner Shareable	X	X	Executed in cluster	
	Outer Shareable	HIGH	X	Output to LLRAM	
		LOW	X	Executed in cluster	
Atomics	Non-shareable	X	HIGH	Executed in cluster	
		X	LOW	Executed in cluster	
	Inner Shareable	X	HIGH	Executed in cluster	
		X	LOW	Executed in cluster	
	Outer Shareable	HIGH	HIGH	Output to LLRAM	
		HIGH	LOW	SLVERR	

Type	Shareability	CFGLLRAMSHARED	BROADCASTATOMICL	Access to LLRAM region	Incoming LLRAM ACP transaction
		LOW	HIGH	Executed in cluster	
		LOW	LOW	Executed in cluster	

The following table describes the support for exclusives and atomics for the following cases:

- Software running from a core within the Cortex®-R82AE processor executing load/store exclusive or atomic instructions accessing the *Main Manager* (MM) region.
- Incoming transactions on the *Main Accelerator Coherency Port* (MACP).



X in the following table means that the value does not have any effect on the exclusives or atomics.

**Table 8-57: Exclusives and atomics support for MM and MACP**

Type	Shareability	BROADCAST signals		Atomic	Access to MM region	Incoming MACP transaction
		OUTERM	ATOMICM			
Exclusives	Non-shareable	X	X	X	Executed in cluster	SLVERR
	Inner/Outer Shareable	HIGH	X	X	Output to MM, if Non-cacheable or Device. Otherwise depends on which cache holds the data.	SLVERR
		LOW	X	X	Output to MM, if Non-cacheable or Device. Otherwise executed in cluster.	SLVERR
Atomics	X	X	X	Near	Executed in cluster	Cannot happen. Atomics from MACP always treated as far.
		X	HIGH	Far	Output to MM	Forward to MM  <b>Note:</b> Non-cacheable atomics are supported. Cacheable atomic transactions return SLVERR.
		X	LOW	Far	SLVERR	SLVERR

## 8.14 Bus timeouts

The Cortex®-R82AE processor implements bus timeout detection, which is a safety feature that can detect timeouts across the four following ports independently for each subordinate.

### *Low-latency Peripheral Port (LLPP) interface timeout*

The LLPP includes a timeout mechanism to detect transactions that fail to complete (that is, LLPP fails to receive a response for incoming requests) within a programmable time limit.

If timeout detection is enabled, the response to a timeout occurrence is:

- For each timeout occurrence, LLPP asserts an error signal by way of *Reliability, Availability, and Serviceability* (RAS).
- If timeout abort is enabled, the transaction failing to complete is aborted and the memory system treats the LLPP as broken. All subsequent transactions targeting the LLPP are aborted.
- Whenever a bus timeout error is detected it is always reported to RAS, with LLPP and MM on Node 7 and SPP and LLRAM on Node 8.
- When a bus timeout occurs on LLPP and timeout abort is enabled, it is not expected that recovery software will be able to fall back to continue execution on other ports.

The timeout limit is determined by setting the IMP\_CPUBUSTIMEOUTR\_EL1.MAXCYCLESBY32LLPP field. To enable the timeout detection, set IMP\_CPUBUSTIMEOUTR\_EL1.ENABLELLPP. To enable the timeout abort, set IMP\_CPUBUSTIMEOUTR\_EL1.ABORTLLPP.

### **Shared Peripheral Port (SPP) interface timeout**

The SPP includes a timeout mechanism to detect transactions that fail to complete (that is, SPP fails to receive a response for incoming requests) within a programmable time limit.

If timeout detection is enabled, the response to a timeout occurrence is:

- For each timeout occurrence, the originating core asserts output signal externally via *Reliability, Availability, and Serviceability* (RAS).
- If timeout abort is enabled, the transaction failing to complete is aborted and the memory system treats the SPP as broken. All subsequent transactions targeting the SPP are aborted.
- Whenever a bus timeout error is detected it is always reported to RAS, with LLPP and MM on Node 7 and SPP and LLRAM on Node 8.
- When a bus timeout occurs on SPP and timeout abort is enabled, it is expected that recovery software will be able to fall back to continue execution using TCMs and LLPP.

The timeout limit is determined by setting the IMP\_CPUBUSTIMEOUTR\_EL1.MAXCYCLESBY32SPP field. To enable the timeout detection, set IMP\_CPUBUSTIMEOUTR\_EL1.ENABLESPP. To enable the timeout abort, set IMP\_CPUBUSTIMEOUTR\_EL1.ABORTSPP.

SPP is on-core basis.

### **Low-latency RAM (LLRAM) interface timeout**

A transaction fails to complete if LLRAM fails to receive a response for incoming requests. LLRAM can also result in a timeout triggered by ACELS subordinate.

If timeout detection is enabled, the response to a timeout occurrence is:

- For each timeout occurrence, the originating core or ACELS asserts output signal *Reliability, Availability, and Serviceability* (RAS).

- If transaction abort is enabled, the transaction failing to complete is aborted by the originating core and the memory system treats the LLRAM interface as broken. All subsequent transactions targeting the LLRAM interface are aborted.
- Whenever a bus timeout error is detected it is always reported to RAS, with LLPP and MM on Node 7 and SPP and LLRAM on Node 8.
- When a bus timeout occurs on LLRAM and timeout abort is enabled, it is expected that recovery software will be able to fall back to continue execution using TCMs and LLPP.

The timeout limit is determined by setting the IMP\_CPUBUSTIMEOUTR\_EL1.MAXCYCLESBY32LLRAM field for each subordinate. To enable the timeout detection, set IMP\_CPUBUSTIMEOUTR\_EL1.ENABLELLRAM. To enable the timeout abort, set IMP\_CPUBUSTIMEOUTR\_EL1.ABORTLLRAM.

### **Main Manager (MM) interface timeout**

The MM includes a timeout mechanism to detect transactions that fail to complete within a programmable time limit, that is, MM fails to receive a response for incoming requests. MM can also get a timeout triggered by MACP subordinate or an internal L2 transaction (for example, HWFLUSH).

A transaction fails to complete if an address or write data beat is not accepted, or a response is not received.

In VMSA there will be no translations if MM has timed out. If timeout detection is enabled, the response to a timeout occurrence is:

- For each timeout occurrence, the originating subordinate core asserts output signal *Reliability, Availability, and Serviceability* (RAS).
- If transaction abort is enabled, the transaction failing to complete is aborted by the originating core and the memory system treats the MM as broken. All subsequent transactions targeting the MM are aborted.
- Whenever a bus timeout error is detected it is always reported to RAS, with LLPP and MM on Node 7 and SPP and LLRAM on Node 8.
- When a bus timeout occurs on MM and timeout abort is enabled, it is expected that recovery software will be able to fall back to continue execution using TCMs and LLPP. Recovery software might be able to continue execution using LLRAM and SPP but this is not guaranteed.

The timeout limit per core is determined by setting the IMP\_CPUBUSTIMEOUTR\_EL1.MAXCYCLESBY32MM field. To enable the timeout detection, set IMP\_CPUBUSTIMEOUTR\_EL1.ENABLEMM. To enable the timeout abort, set IMP\_CPUBUSTIMEOUTR\_EL1.ABORTMM.

## 8.15 Real-time considerations

The Cortex®-R82AE processor provides mechanisms and registers to ensure that your system can meet various real-time requirements.

This section describes the conditions, mechanisms, and register controls for the Cortex®-R82AE processor so that your system can achieve:

- Bounded interrupt latency response under the best-case and worst-case conditions
- Hierarchical real-time requirements on interfaces and memories
- Quality of service capabilities to prioritize a core or a complete cluster.



The `DC ISW`, `DC CSW` and `DC CISW` instructions for the L1 data cache are serialized through the L2 cache. To ensure that *Low-latency RAM* (LLRAM) accesses cached through the L1 caches have higher real-time response than the *Main Manager* (MM) accesses, Arm recommends that you do not use these instructions for critical software sections.

### 8.15.1 Interrupt latency

The Cortex®-R82AE processor guarantees a bounded interrupt latency response provided that your system and software meet certain conditions.

The Cortex®-R82AE processor has an interrupt latency of 60 SCLK cycles under best-case interrupt latency conditions and 120 SCLK cycles under worst-case interrupt latency conditions.

Interrupt latency refers to the number of SCLK cycles from the assertion of a *Shared Peripheral Interrupt* (SPI) pin to the cycle in which the instruction before the first non-generic instruction in the interrupt handler retires. This includes the time for the execution of the instructions for identifying the interrupt, branching to the specific interrupt handler, stacking the relevant registers, and clearing the interrupt mask.

This section describes the conditions that your system and software should fulfill for the Cortex®-R82AE processor to achieve the best-case and worst-case interrupt latency cycles.

#### 8.15.1.1 Interrupt handler

The interrupt handler code can greatly affect the interrupt latency of your system.

The Cortex®-R82AE processor accepts and processes interrupts within 60 and 120 SCLK cycles, if your interrupt handler meets the following conditions:

- The interrupt is handled by the target Exception level. In other words, the interrupt is not trapped by the hypervisor to route it to a virtual machine which can handle the interrupt.



- The related exception vector and interrupt handler code belong to *Memory Protection Unit* (MPU) regions of 4KB or larger.
- There is a first, generic part of the handler, that is common for all interrupts. This part is written in Assembly. The code is optimized to take advantage of the processor multi-issuing capabilities.
- There is a second, non-generic part of the handler, that depends on the interrupt ID. This part may be written either in Assembly or a higher-level language, such as C.
- The generic handler stacks general-purpose registers. The generic handler does not stack NEON/FP registers. It is assumed that the non-generic handler does not use NEON/FP instructions.
- The generic handler acknowledges the highest-priority interrupt and reads its interrupt ID.
- The generic handler re-enables (unmasks) interrupts as soon as possible, so that higher-priority interrupts can be taken.
- The generic handler looks up the interrupt ID from a table in memory and finds out which non-generic handler function must be called.
- The generic handler calls the non-generic handler to service the specific interrupt.
- The generic handler is executed from the *Instruction Tightly Coupled Memory* (ITCM).
- The generic handler uses the handler-specific stack which is in the *Data Tightly Coupled Memory* (DTCM).
- The generic handler does not perform any access to the *Main Manager* (MM) port, *Low-latency RAM* (LLRAM) port, *Low-latency Peripheral Port* (LLPP), and *Shared Peripheral Port* (SPP).
- The generic handler does not perform any exclusive or atomic memory access.

An example of such a generic handler for EL1 IRQs, from the vector entry up to the function call of the non-generic handler, is given in [D.1 Generic handler example, part 1](#) on page 2305.

An example of the remainder of the generic handler, from the return of the non-generic handler function up to the exception return is given in [D.2 Generic handler example, part 2](#) on page 2306.

Using this example handler as a reference, the best-case and worst-case interrupt latency is measured from the cycle when the SPI IRQ pin of the GIC is asserted, up to the cycle when the first instruction of the function called by the BLX X3 instruction has retired.

### 8.15.1.2 Best-case interrupt latency conditions

Under best-case interrupt latency conditions, the interrupt is accepted as soon as it is received by the core within the Cortex®-R82AE processor. There cannot be ongoing interrupts or operations such as Device, atomic, or exclusive operations that would delay the interrupt handling.

The Cortex®-R82AE processor accepts and processes the interrupt within 60 SCLK cycles if your system and software meet the following conditions:

- The *Generic Interrupt Controller* (GIC) distributor used is an Arm product supporting functional safety and real-time interrupts, such as GIC-720AE

- The GIC distributor is clocked at half the frequency as the Cortex®-R82AE cluster, with no bus bridges between the two.
- The GIC redistributor has enabled combined packets (GICR\_FCTLR.ECP field is set to 1).
- The *Shared Peripheral Interrupt* (SPI) which is asserted is a low-latency targeted SPI (the related GICD\_IROUTER<n>.IRM field is set to 0).
- Interrupt configuration (routing, priority, group assignment, per-interrupt enables, group enables, exception vector) is static.
- The level interrupts are not deasserted before they are serviced.
- Any number of SPIs are allowed to be asserted at the same time for the same core with any priority structure. Interrupts are not delivered to any other cores in the cluster.
- Data memory barrier instructions and instructions that write to memory with release semantics do not delay interrupts. That is, either of the following applies:
  - An EL0 or EL1 source context takes an interrupt to an EL2 destination context.
  - Such instructions are not being present in the source context.
  - IMP\_CPUACTLR\_EL1.DMB bit is set which enables such instructions to be interruptible.
- The memory translation regime at the target Exception level uses PMSAv8-64.
- There are no ongoing accesses to debug or trace functions, *Reliability, Availability, and Serviceability* (RAS) registers, *Performance Monitoring Unit* (PMU), or timer registers.
- The targeted core is not in the process of correcting an *Error Correcting Code* (ECC) error. A bus timeout has not occurred for the targeted core.
- The cluster and the targeted core are powered up and that the core clock SCLK is running. In other words, the core is not executing a *WFI* or *WFE* instruction.
- Exception-handling software is not using implicit error synchronization events, that is SCTLX\_ELx.IESB is assumed to be 0b0.
- No core in the cluster is sending *Software Generated Interrupts* (SGI).
- No external agent (such as a DMA engine) is accessing the targeted core's *Tightly Coupled Memories* (TCMs) through the *ACE-Lite Subordinate* (ACELS) port. No Online MBIST testing is being performed for the memories of the targeted core.
- No external agent (such as a DMA engine) is accessing the targeted core's *Low-latency RAM* (LLRAM) interface through the ACELS port.
- The targeted core is not in the process of handling another interrupt.
- No core in the cluster is performing any Device memory accesses.
- No core in the cluster is performing any atomic operations.
- No core in the cluster is performing any exclusive operations.

### 8.15.1.3 Worst-case interrupt latency conditions

Worst-case interrupt latency conditions allow for the interrupt recognition to be delayed.

This may occur because:

- The core is executing a Device, atomic or exclusive operation.
- The core currently handling an interrupt and therefore masking new interrupts.
- Interrupts are being delivered to other cores in the cluster.

The Cortex®-R82AE processor accepts and processes the interrupt within 120 SCLK cycles if your system and software meet the following conditions:

- The GIC distributor used is GIC-625.
- The GIC distributor is clocked at half the frequency as the Cortex®-R82AE cluster, with no bus bridges between the two.
- PERIPHCLK is clocked at 25% or higher of the SCLK frequency.
- The *Shared Peripheral Interrupt* (SPI) which is asserted is a low-latency targeted SPI.
- Interrupt configuration (routing, priority, group assignment, per-interrupt enables, group enables, exception vector) is static.
- The level interrupts are not deasserted before they are serviced.
- Data memory barrier instructions and instructions that write to memory with release semantics do not delay interrupts. That is, either of the following applies:
  - An EL0 or EL1 source context takes an interrupt to an EL2 destination context.
  - Such instructions are not being present in the source context.
  - IMP\_CPUACTLR\_EL1.DMB bit is set which enables such instructions to be interruptible.
- The memory translation regime at the target Exception level uses PMSAv8-64.
- There are no ongoing accesses to debug or trace functions, RAS registers, or PMU registers.
- The targeted core is not in the process of correcting an *Error Correcting Code* (ECC) error. A bus timeout has not occurred for the targeted core.
- Any core in the cluster can be executing a *WFI* or *WFE* instruction, in which case they may have their clock being architecturally gated. However, the Cortex®-R82AE processor SCLK must be active. This can be achieved by setting IMP\_CLUSTERACTLR\_EL1.SCLKQ to 0b1.
- Exception-handling software is not using implicit error synchronization events, that is SCTLX\_ELx.IESB is assumed to be 0b0.
- Cores in the cluster are allowed to send *Software Generated Interrupts* (SGI).
- External agents (such as a DMA engine) are allowed to be accessing any core's TCM memories through the *ACE-Lite Subordinate* (ACELS) port.
- External agents (such as a DMA engine) are allowed to be accessing any core's *Low-latency RAM* (LLRAM) interface through the ACELS port. No Online MBIST testing is being performed for the memories of the targeted core.
- Cores are allowed to perform Device memory accesses. Device memory accesses are only performed through the *Low-latency Peripheral Port* (LLPP) or the *Shared Peripheral Port* (SPP) and not through the LLRAM or *Main Manager* (MM) ports. Device memory accesses do not span the 128-bit boundary for the LLPP and 64-bit boundary for the SPP.

- Cores are allowed to perform Atomic operations. Atomic operations may be performed through the LLRAM or MM ports but they must be configured to perform them as near atomics. This is done by setting the IMP\_CPUACTLR\_EL1.ATOM bit field to 0b01.
- Cores are allowed to perform Exclusive operations. Exclusive operations may be performed through the LLRAM or MM ports, but they must be configured to be cacheable within the cluster (The *Memory Protection Unit* (MPU) regions are programmed as cacheable and Inner Shareable).
- Atomic and exclusive operations are allowed to be performed to the *Tightly Coupled Memories* (TCMs). Such operations cannot be used for inter-core communication because the TCM regions are private to each core.
- The system components attached to the Cortex®-R82AE processor manager ports respond in a timely fashion. That is, the components are clocked synchronously to SCLK with a 2:1 clock ratio; the components can handle pipelined transactions; and the components respond within 3 clock cycles.
- There can be any number of cores in the cluster (up to the maximum of eight cores). Interrupts can be under delivery to any number of cores in the cluster.
- SPIs can be asserted at the same time which target any number of cores within the cluster.
- Ongoing accesses to timer registers are allowed.
- The new interrupt, for which the latency is measured, has higher priority than any other ongoing interrupt that is being processed.

The worst-case interrupt latency conditions assume that the software running on the Cortex®-R82AE processor fulfills the conditions set above for getting 120 SCLK cycle interrupt response. To ensure these conditions are met, the hypervisor running at EL2 can enforce the EL1 and EL0 software to achieve some of those conditions.

- Setting the IMP\_INTLATENCY\_EL2.DEV bit to 0b1 forces any Device access on the LLRAM or MM ports to abort.
- Setting the IMP\_INTLATENCY\_EL2.DEV bit to 0b1 forces any Device memory access where all bytes are not within a 128-bit aligned region on the LLPP or a 64-bit aligned region on the SPP to abort.
- Setting the IMP\_INTLATENCY\_EL2.ATOM bit to 0b1 forces atomics either to be near or to abort if they cannot be executed near.
- Setting the IMP\_INTLATENCY\_EL2.EXCL bit to 0b1 forces exclusives that cannot be contained in the cluster to abort.
- The EL2 MPU region programming can also override EL1 MPU region programming.

See the [A.2.2.109 IMP\\_INTLATENCY\\_EL2, Interrupt Latency Register](#) on page 749 for more information.

## 8.15.2 Real-time hierarchy

The Cortex®-R82AE processor provides various memories and interfaces each tailored to different real-time requirements. The aim is that some memories and interfaces are used for more critical real-time requirements and some for less critical real-time requirements.



Note

The more real-time critical context is also able to access the less real-time critical interfaces and memories although such an access might not be desirable depending on the system design.

The Cortex®-R82AE processor memories and interfaces can be ordered as follows in terms of meeting the critical real-time requirements:

1. The *Tightly Coupled Memories* (TCMs) and the *Low-latency Peripheral Port* (LLPP) are suitable for meeting the most critical real-time requirements.
2. The *Low-latency RAM* (LLRAM) port, cached through the L1 caches, and the *Shared Peripheral Port* (SPP) are suitable for meeting the medium critical real-time requirements. They are more deterministic than the *Main Manager* (MM) but less deterministic than the TCMs and the LLPP.
3. MM, cached through the L1 and L2 caches, is suitable for meeting the least critical real-time requirements. MM is the least deterministic.

To ensure that the LLRAM and the SPP accesses meet higher real-time requirements compared to the MM accesses, the Cortex®-R82AE processor provides a mechanism to reserve buffers for the LLRAM and SPP accesses. Reserving certain buffers specifically for LLRAM and SPP accesses avoids the cases where all the buffers are in use for the MM accesses while the software tries to access the LLRAM or the SPP, therefore avoids the need to wait for ongoing MM accesses to complete.

If the Cortex®-R82AE processor has the LLRAM port and the SPP implemented and if your system always requires the LLRAM and SPP accesses to have higher real-time response than the MM accesses:

- The EL1 software should set the `IMP_CPUACTLR_EL1.LCURES` to `0b1` to reserve buffer slots and linefill descriptors to ensure that the LLRAM and SPP accesses do not have increased worst case latency caused by MM accesses.
- Hypervisor software running at EL2 can also set the `IMP_INTLATENCY_EL2.LCURES` to `0b1` to ensure that the EL1 software treats the `IMP_CPUACTLR_EL1.LCURES` as `0b1` regardless of its actual value.

The default values for `IMP_CPUACTLR_EL1.LCURES` and `IMP_INTLATENCY_EL2.LCURES` bits are `0b0`. If your system requires the LLRAM and SPP accesses to be always prioritized over MM accesses, consider setting some of these bits to `0b1`, according to your needs.

See [A.2.2.44 IMP\\_CPUACTLR\\_EL1, CPU Auxiliary Control Register](#) on page 542 and [A.2.2.109 IMP\\_INTLATENCY\\_EL2, Interrupt Latency Register](#) on page 749 for more information.

### 8.15.3 Freedom from Interference

This section details how the Cortex®-R82AE processor can be used to create systems which achieve freedom from interference.

#### 8.15.3.1 Temporal Freedom from Interference

A system achieves temporal freedom of interference when it enables each system task to meet response time deadlines by providing predictable and timely access to critical system resources, such as computation, memory and peripherals.

The Cortex®-R82AE processor will aim to ensure freedom of interference between different contexts where possible, where freedom of interference is defined as the ability for a more deterministic context to make forward progress without dependencies on less deterministic contexts. In particular a real-time context should be free of any interference from a context running a rich guest OS. When multiple real time contexts exist within a system it is also possible for there to be dependencies between them depending on the system design.

The Cortex®-R82AE processor supports multiple memory ports which provide differing levels of determinism, for the purpose of describing how to achieve temporal freedom from interference the following three usage models are described in this section:

1. Non real-time context, which uses the main manager (MM) port for Normal memory accesses, and the shared peripheral port (SPP) for Device memory accesses. A non real-time context can use VMSA or PMSA.
2. Partially real-time context, which uses the low-latency RAM (LLRAM) port for shared Normal memory accesses, tightly-coupled memories (TCM) for non-shared Normal memory accesses, SPP for access to shared peripherals with Device memory accesses and the low-latency peripheral port (LLPP) for access to peripherals private to the core. A partially real-time context can only use PMSA.
3. Fully real-time context, which only uses TCM for Normal memory accesses and LLPP for Device memory accesses. This provides the most deterministic execution. A fully real-time context can only use PMSA.

A context refers to either software running at EL1 and EL0 with a given value of VSCTLR\_EL2.VMID set or software running at EL2. All software running at EL2 is within the same context. If a system uses multiple contexts, switching between them is expected to be controlled by a hypervisor at EL2. For a system that does not utilize EL2 it is expected that only a single context is executed and so freedom from interference between contexts does not apply.

When developing software or systems using the Cortex®-R82AE processor, it should be noted:

- The architecture only guarantees that a single PE in the system makes forward progress with an exclusive sequence. Exclusives are unlikely to be suitable when it is required that all exclusive threads make forward progress. This is due to the architecture of exclusive sequences and is not specific to the Cortex®-R82AE processor. It is recommended to use atomics instead to implement synchronization primitives such as semaphores.

- When software meets the assumptions of use for freedom from interference, it will ensure that a more deterministic context does not have a dependency on a less deterministic context. However, a less deterministic context may still affect the performance of a more deterministic context.
- By dedicating a context to a particular core, performance may be improved as more resources are available to that context. This can also allow improved fault containment, as if only a single context is running on a core any asynchronous faults that occur can be contained to that context.
- As freedom from interference is a superset of the requirements to guarantee interrupt latency, not all types of instruction can be used. For example, non-cacheable atomics cannot be interrupted and so it is not possible to guarantee freedom from interference when they are used. This means that not all types of instruction are available for sharing data while guaranteeing freedom from interference.

### 8.15.3.2 Temporal freedom from interference between a rich context and a partially real-time context

This section details how the Cortex®-R82AE processor can be used to create systems which achieve temporal freedom from interference between a rich context and a partially real-time context.

Freedom from interference between a rich context from partially real-time context will be achieved if your system and software meets the following conditions:

- A partially real-time context does not use the MM port.
  - The MM port is not designed to provide freedom from interference from other cores and from dependencies in the system.
  - Any VMSA memory access will have an implicit dependency on the MM port, so a partially real-time context must only use PMSA.
  - This includes not executing DC and IC instructions associated with MM addresses.
  - This includes not executing IC IALL{US}, or any TLBI instructions.
  - Any context that uses MM and executes a DSB SY will depend on previous instruction cache and TLB maintenance performed in any context.
  - Enforcement: This can be enforced using the stage 2 MPU, IC IALL{US} instructions can be prevented by setting IMP\_INTLATENCY\_EL2.MMDVM and TLBI instructions can be prevented by setting HCR\_EL2.TTLB.
- Memory is not shared between contexts, unless following all the assumptions for how to share data between contexts.
  - Enforcement: This can be enforced using the stage 2 MPU and setting IMP\_INTLATENCY\_EL2.MMDVM.
- The LLRAM port is connected to a simple SRAM, or the system otherwise ensures LLRAM transactions are always able to make forward progress without depending on other less deterministic transactions in the system.
  - Enforcement: This must be enforced by the system designer.

- Peripherals connected to the SPP and LLPP shall not share resources with other buses in the system or otherwise ensure that SPP and LLPP transactions are always able to make forward progress without depending on other less deterministic transactions in the system.
  - Enforcement: This must be enforced by the system designer.
- The IMP\_CPUACTLR\_EL1.DMB or IMP\_INTLATENCY\_EL2.DMB bit is set to upgrade Data Memory Barrier (DMB) instructions into a Data Synchronization Barrier (DSB) allowing it to be flushed on a context switch and so not delay execution of barriers in the new context.
  - Enforcement: This can be enforced by IMP\_INTLATENCY\_EL2.DMB
- Set/way maintenance of the L1 data cache is not used as this introduces a dependency on the MM port.
  - Enforcement: This can be enforced by HCR\_EL2.TSW.
- The IMP\_CPUACTLR\_EL1.LCURES or IMP\_INTLATENCY\_EL2.LCURES bit is set.
  - Enforcement: This can be enforced by setting IMP\_INTLATENCY\_EL2.LCURES
- Software follows the assumptions of use for worst-case interrupt latency conditions.
- There are no ECC errors
- There are no bus timeouts on LLRAM
  - It is expected that recovery software can run using TCM and LLPP after a bus timeout, but it is not expected that real-time contexts will be able to continue to run as it is likely not to be possible to perform a context switch after a bus timeout has occurred.
  - When a bus timeout occurs, it is not expected that the old context will be saved and so it is not possible to return to the context in which the bus timeout occurred and further accesses to LLRAM will abort.
- Assumes that all cores in the cluster follow assumptions on freedom from interference

### 8.15.3.3 Temporal freedom of interference between a fully real-time context and less deterministic contexts

This section details how the Cortex®-R82AE processor can be used to create systems which achieve temporal freedom from interference.

Freedom from interference between a fully real-time context and less deterministic contexts will be achieved if your system and software meets the following conditions:

- A fully real-time context only uses the TCM and LLPP ports.
  - Enforcement: This can be enforced using the stage 2 MPU, or by disabling the regions in the region registers and removing write access to the region registers.
- Memory is not shared between contexts, unless following all the assumptions for how to share data between contexts.
  - Enforcement: This can be enforced using the stage 2 MPU.
- Peripherals connected to the LLPP shall not share resources with other buses in the system or otherwise ensure that LLPP transactions are always able to make forward progress without depending on other less deterministic transactions in the system.



- Enforcement: This must be enforced by the system designer.
- The IMP\_CPUACTLR\_EL1.DMB or IMP\_INTLATENCY\_EL2.DMB bit is set to upgrade Data Memory Barrier (DMB) instructions into a Data Synchronization Barrier (DSB) allowing it to be flushed on a context switch and so not delay execution of barriers in the new context.
  - Enforcement: This can be enforced by IMP\_INTLATENCY\_EL2.DMB.
- Maintenance of caches or TLBs are not performed.
  - Enforcement: This can be enforced by setting all of HCR\_EL2.{TTLB, TPU, TPCP, TSW}.
- Software follows the assumptions of use for worst-case interrupt latency conditions.
- There are no bus timeouts on LLPP.
  - It is expected that recovery software can run using TCM and LLPP after a bus timeout, but it is not expected that real-time contexts will be able to continue to run as it is likely not to be possible to perform a context switch after a bus timeout has occurred.
  - When a bus timeout occurs, it is not expected that the old context will be saved and so it is not possible to return to the context in which the bus timeout occurred and further accesses to LLPP will abort.
- Assumes that all cores in the cluster follow assumptions on freedom from interference.

#### 8.15.3.4 Ensuring temporal freedom of interference in a hypervisor

This section details how the Cortex®-R82AE processor can be used to create systems which achieve temporal freedom from interference when using a hypervisor to manage contexts.

Freedom from interference when a hypervisor is present will be achieved if your system and software meets the following conditions:

- The hypervisor follows all assumptions to ensure freedom from interference according to the memory ports used by the hypervisor.
  - When the hypervisor is only using TCM and LLPP, assumes the hypervisor follows all assumptions to ensure freedom from interference from a fully real-time context from other contexts.
  - When the hypervisor is also using LLRAM and/or SPP, assumes the hypervisor follows all assumptions to ensure freedom from interference from a partially real-time context from other contexts.
  - Assumes that the hypervisor does not use the MM port. It is possible to use the MM port to boot from, then branch to execution from another port and execute a DFB instruction. When the DFB instruction is completed it is then possible to achieve freedom from interference.
- The Data Full Barrier (DFB) instruction is not used unless the software after the DFB does not rely on freedom from interference.
  - DFB will depend on all previous memory accesses but is interruptible, so only creates a dependence for the instructions after it in program order and if there is an interrupt the DFB will be flushed and so not create any dependencies. Once the DFB instruction is completed it has no impact on freedom from interference.

- AT operations for EL1/0 are not executed in EL2 when the VTCR\_EL2.MSA bit is set.
  - This will introduce dependencies on MM by executing a pagewalk.
- The hypervisor does not execute cache debug operations and ensures ACTLR\_EL2.CDBG is cleared.
- The hypervisor only switches between two contexts on a given core.
- The hypervisor sets the IMP\_INTLATENCY\_EL2.LCUDVM bit when non real-time contexts are executing to prevent introducing dependencies when data is shared between different contexts.
- The hypervisor sets the IMP\_INTLATENCY\_EL2.MMDVM bit when real-time contexts are executing to prevent introducing dependencies when data is shared between different contexts.
- The hypervisor disables bus timeout aborting behavior for ports that are not in use when switching to a new context.
  - For example, when switching to a real-time context the hypervisor should disable aborting behavior for bus timeouts on MM. Any bus timeouts for not currently active contexts will be reported in the RAS registers.

#### 8.15.3.5 Ensuring temporal freedom of interference while sharing data

This section details how the Cortex®-R82AE processor can be used to create systems which achieve temporal freedom from interference while sharing data.

Freedom from interference while sharing data between different contexts will be achieved if your system and software meets the following conditions:

- Data is only shared between the following pairs of contexts:
  - Between a non-real time and a partially real-time context using the LLRAM port.
  - Between a partially real-time and a fully real-time context using TCMs.
- Instruction cache maintenance is not performed to the LLRAM port when sharing data using the LLRAM port on the same core.
  - Enforcement: This can be enforced by setting IMP\_INTLATENCY\_EL2.LLRAMDVM.

Freedom from interference while sharing data between different real-time and non real-time contexts can be performed without introducing dependencies by using one of the following methods:

- The non real-time context executes writes into the LLRAM memory by performing writes to the MM port targeting the ACELS-LLRAM via a loopback in the system.
  - Note: this requires functionality provided by the system.
  - Enforcement: This can be enforced by the stage 2 MPU.
- Contexts are statically allocated to cores such that all contexts on a given core have the same real-time requirements.

- For example, one core can be executing a rich OS which also produces some data, written to LLRAM, to be consumed by a partially real-time context. The consumer is allocated to a different core which reads from this same location from the LLRAM port.
- Enforcement: This can be enforced by the hypervisor.
- The non real-time context uses LLRAM to read or write data, without performing instruction cache maintenance for LLRAM addresses.
  - Enforcement: This can be enforced by setting IMP\_INTLATENCY\_EL2.LLRAMDVM.

### 8.15.4 Quality of Service

You can prioritize memory accesses from a specific core over accesses from the other cores within the Cortex®-R82AE processor. Similarly, you can also prioritize the Cortex®-R82AE cluster over the other clusters within your system.

You can set priority options for a core or for the whole cluster with the IMP\_CLUSTERQOSR\_EL1 register.

Setting the IMP\_CLUSTERQOSR\_EL1.COREQOSEN to 0b1 enables *Quality of Service* (QOS) within the Cortex®-R82AE processor. When this bit is set to 0b1, you can set which core is prioritized by setting the IMP\_CLUSTERQOSR\_EL1.COREQOSID bits. The COREQOSID bitfield has no effect if the COREQOSEN is 0b0.

When QOS is enabled for a specific core, the *Low-latency RAM* (LLRAM), the *Shared Peripheral Port* (SPP), and the L2 cache accesses from that core have higher priority over the accesses from the other cores within the Cortex®-R82AE processor.

IMP\_CLUSTERQOSR\_EL1.CLQOS controls the priority over other clusters within your system. This field is driven by the *Main Manager* (MM) ARQOSM and AWQOSM QOS signals. Your interconnect should support prioritization of clusters if your system requires the QOS to be set for the whole cluster.

See [A.2.2.60 IMP\\_CLUSTERQOSR\\_EL1, Cluster Quality of Service Register](#) on page 608 for more information.

## 9. Memory management

This chapter describes how the memory space of the Cortex®-R82AE processor is managed.

### 9.1 About the memory management

The Cortex®-R82AE processor memory management system determines various attributes for each memory location including access permissions, memory types, and Cacheability.

Access permissions indicate which levels of privilege are permitted to access a location and whether write access or instruction execution are permitted. Memory type and Cacheability attributes affect the way the Cortex®-R82AE processor handles particular accesses, for example, whether or not it permits two stores to be merged into a single write access.

Each core within the Cortex®-R82AE processor has two programmable *Memory Protection Units* (MPUs) and an optional *Memory Management Unit* (MMU):

- The EL1 MPU is controlled by operating system software running at EL1. The EL1 MPU enables isolation between applications running at EL0.
- The EL2 MPU is controlled by hypervisor software running at EL2. The EL2 MPU enables isolation between operating systems running at EL1.
- Optional EL1 MMU is controlled by operating system software running at EL1. The EL1 MMU enables address translation and isolation between applications running at EL0.

The MPU implements the *Protected Memory System Architecture* (PMSA) and MMU implements the *Virtual Memory System Architecture* (VMSA).

PMSA has no address translation capabilities. Therefore the physical address is always the same as the virtual address for the MPU.

VMSA has address translation capabilities and is responsible for translating virtual addresses into physical addresses.



Virtual address refers to the address before the translation process as generated by the instruction. Physical address refers to the address after the translation process as visible on the bus.

---

EL2 software goes through one stage of EL2 MPU translation. EL1 and EL0 software go through one stage of either EL1 MPU or EL1 MMU translation optionally followed by one stage of EL2 MPU translation.



- If the EL1 MMU is not included, then the EL1 MPU has non zero regions. If the EL1 MMU is included, then the EL1 MPU is optional.
- EL2 MPU programmable regions are optional. The value 0 for MPU region indicates that the core does not support any programmable regions for this MPU. Note however that default or architectural memory maps may still be used.

The Cortex®-R82AE processor memory management architecture enables virtualization of operating systems. Hypervisor software running on EL2 selects between the MPU and MMU on a per-operating system basis.

The Cortex®-R82AE processor always operates in Secure state and all translation regimes are Secure. However, the Cortex®-R82AE processor is able to access both Secure and Non-secure address space. The Cortex®-R82AE processor MPU regions and MMU pages include configurable attributes that determine whether accesses to addresses within a region or page are to the Secure or Non-secure address space.

Memory management system translation results are cached to reduce translation costs on performance and power. Each core within the Cortex®-R82AE processor includes an L1 instruction cache structure (L1I MMS) and an L1 data cache structure (L1D MMS) that contain the results of memory management system lookups. An access that hits in the L1I MMS or L1D MMS incurs no extra latency.

Each core within the Cortex®-R82AE processor that supports VMSA includes a L2 *Translation Lookaside Buffer* (TLB) that contains the results of page table walks.

## 9.2 MPU

Each core within the Cortex®-R82AE processor has two programmable *Memory Protection Units* (MPUs), controlled from EL1 and EL2. Depending on the parameter PA\_W, each MPU supports a 40-bit (when PA\_W=40) or a 48-bit (PA\_W=48) physical address range that allows up to 1TB and 256TB memory address range, respectively, to be subdivided into regions.

Each memory region is defined by a base address, limit address, access permissions, and memory attributes.

For data accesses, the MPU checks that the type of access (read or write) to a region is allowed for the current translation regime. For instruction accesses, the MPU checks if an access is allowed to the region and that the translation regime allows execution. For both data and instruction accesses, if access is allowed, the MPU assigns the memory attributes defined for the region. If access is not allowed, a permission fault is taken. A translation fault is taken for the following reasons:

- If an access hits in more than one region in one of the MPUs.
- If an access does not hit in any MPU region and the Background region cannot be used (based on the MPU configuration and current privilege level).



A translation fault is only taken when the MPU is enabled in software.

As a result of pipelined operation, the Cortex®-R82AE processor tries to predict program flow and future data accesses, and so it fetches data and instructions ahead of their use. These transactions are known as speculative transactions until the pipeline completes execution of the corresponding instruction. This might result in the Cortex®-R82AE processor generating addresses either outside permitted regions or not having privilege to attempt the access. In these cases, speculative accesses are prevented from generating bus transactions by the MPU but do not raise a translation or permission fault.

Each core within the Cortex®-R82AE processor has an EL1-controlled MPU and an EL2-controlled MPU with 0, 16, or 32 programmable regions. The value 0 indicates that the core does not include support for MPU for any programmable regions, but software can still make use of architectural/default memory maps. For the EL1-controlled MPU, the value 0 is supported only when the core includes support for *Memory Management Unit* (MMU).

When the EL2-controlled MPU and virtualization are enabled, all transactions using the EL0/EL1 translation regime perform a lookup in both MPUs. The resulting attributes are combined so that the least permissive attributes are taken. These two stages of protection allow the hypervisor to retain control over the EL0/EL1 translation regime and therefore enables support for virtualization. When software executes using the EL2 translation regime, only the EL2-controlled MPU is used.

For more information on the MPU, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

## 9.2.1 MPU regions

A region is a contiguous range of addresses starting at a base address, extending up to and including a limit address.

The Cortex®-R82AE processor *Memory Protection Unit* (MPU) region address ranges are defined as a pair with base and limit addresses. These addresses are arbitrary except for a minimum 64-byte resolution. This provides flexibility and reduces the number of regions that are required to fully describe a memory map compared to older versions of the Arm architecture.

The base address is configured by PRBAR\_EL1 (PRBAR\_EL2 for EL2-controlled MPU) and the limit address is configured by PRLAR\_EL1 (PRLAR\_EL2 for EL2-controlled MPU). The base address is aligned on a 64-byte boundary and the limit address is aligned to the byte below a 64-byte boundary. For the remainder of this section, short terms such as PRBAR are used to describe any of the EL1 or EL2 MPU registers (PRBAR\_EL1, PRBAR\_EL2, PRBAR<n>\_EL1, PRBAR<n>\_EL2).

Both base and limit addresses are inclusive, meaning that an address within a region is given by:

```
PRBAR.BASE:0b000000 <= address <= PRLAR.LIMIT:0b111111
```

Where : is a bit concatenation operator.

The minimum size for a region is 64 bytes.

The Cortex®-R82AE processor implements a parameterized physical address width, and can be either 40 (when parameter PA\_W=40) or 48 (when parameter PA\_W=48).



Even though the minimum resolution that can be programmed in the MPU region is 64 bytes, the Cortex®-R82AE processor is optimized for a minimum region size of 4KB. Any region smaller than 4KB may incur additional cycles of latency for instruction fetches, loads, and stores.

The Cortex®-R82AE processor MPU regions support programming through System register operations. Both an indirect method (for example through PRSELR\_EL1/PRBAR\_EL1/PRLAR\_EL1) and a direct method (for example through PRBAR<n>\_EL1/PRLAR<n>\_EL1) are provided. This allows software to be optimized for either code density or faster reprogramming and context switching.

PRBAR and PRLAR also hold the access permissions (PRBAR.AP), Shareability (PRBAR.SH), the Execute-never bit (PRBAR.XN), and memory attribute index (PRLAR.AttrIdx).

Memory attributes are determined by indexing the *Memory Attribute Indirection Registers* (MAIR\_ELx) with PRLAR.AttrIdx.

A region is enabled or disabled by setting or clearing the region enable bit (PRLAR.EN). In the EL1-controlled and EL2-controlled MPUs, regions can also be enabled or disabled by writing to the *MPU Region Enable Register* (PRENR\_EL1 or PRENR\_EL2).

Speculative memory accesses can occur as a result of prefetching instructions or predicting data accesses. The Cortex®-R82AE processor only speculates on Normal memory, and does not speculate on Device memory. If your system needs to avoid speculative accesses for certain address regions, ensure that the combined effect from MPU programming, Background region, and the related system control bits result in these address regions either producing a fault or assigning a Device memory attribute.

### 9.2.1.1 EL1-controlled MPU Background region

When the EL1-controlled *Memory Protection Unit* (MPU) is disabled (SCTLR\_EL1.M=0):

- If SCTLR\_EL1.BR =1, the EL1 default memory map (MPU Background region) is used as it is shown in [Table 9-1: EL1-controlled MPU Background region - instruction access and data access](#) on page 220.
- If SCTLR\_EL1.BR =0, the Arm®v8-A AArch64 Memory View is used.

When the EL1-controlled MPU is enabled (SCTLR\_EL1.M=1), the MPU Background region can be enabled by setting SCTLR\_EL1.BR. In this case, accesses from the EL1 translation regime that do not hit any programmable regions use the EL1-controlled MPU Background region.

The complete EL1-controlled MPU Background region is always Secure, that is, Non-secure (NS) bit is 0.

The following table shows the EL1-controlled MPU Background region for both instruction access and data access.

**Table 9-1: EL1-controlled MPU Background region - instruction access and data access**

Region	Address range	Attributes	Execute-never (XN) bit
0	0x00000000–0x3FFFFFFF	Normal,  Inner Write-Back,  Inner Read-Allocate,  Inner Write-Allocate,  Outer Write-Back,  Outer Read-Allocate,  Outer Write-Allocate,  Outer Shareable	0
1	0x40000000–0x7FFFFFFF	Normal,  Inner Write-Through,  Inner Read-Allocate,  Inner Write-Allocate,  Outer Write-Through,  Outer Read-Allocate,  Outer Write-Allocate,  Outer Shareable	0
2	0x80000000–0xFFFFFFFF	Normal,  Inner Non-cacheable,  Outer Non-cacheable,  Outer Shareable	1
3	0x000100000000–0x00FFFFFFFF	Device-nGnRnE	1



Access permission for all regions and address ranges is 0b00. Access permission 0b00 implies that the EL1 MPU Background region provides both read and write access to accesses from EL1 translation regime that hit any region in the EL1 MPU Background region.

Any accesses from EL0 that hit in EL1 MPU Background region have no read/write access and generate permission fault.

### 9.2.1.2 EL2-controlled MPU Background region

When the EL2-controlled *Memory Protection Unit* (MPU) is disabled (SCTLR\_EL2.M=0):

- If SCTLR\_EL2.BR =1, the EL2 default memory map (MPU Background region) is used as it is shown in [Table 9-2: EL2-controlled MPU Background region - instruction access and data access](#) on page 221.
- If SCTLR\_EL2.BR =0, the Arm®v8-A AArch64 Memory View is used.

When the MPU is enabled (SCTLR\_EL2.M=1), the MPU Background region can be enabled by setting SCTLR\_EL2.BR. In this case, accesses from the EL2 translation regime that do not hit any programmable regions use the EL2-controlled MPU Background region.

The complete EL2-controlled MPU Background region is always Secure, that is, Non-secure (NS) bit is 0.

The following table shows the EL2-controlled MPU Background region for both instruction access and data access.

**Table 9-2: EL2-controlled MPU Background region - instruction access and data access**

Region	Address range	Attributes	Execute-never (XN) bit
0	0x00000000–0x3FFFFFFF	Normal,  Inner Write-Back,  Inner Read-Allocate,  Inner Write-Allocate,  Outer Write-Back,  Outer Read-Allocate,  Outer Write-Allocate,  Outer Shareable	0

Region	Address range	Attributes	Execute-never (XN) bit
1	0x40000000–0x7FFFFFFF	Normal,  Inner Write-Through,  Inner Read-Allocate,  Inner Write-Allocate,  Outer Write-Through,  Outer Read-Allocate,  Outer Write-Allocate,  Outer Shareable	0
2	0x80000000–0xFFFFFFFF	Normal,  Inner Non-cacheable,  Outer Non-cacheable,  Outer Shareable	1
3	0x000100000000–0x00FFFFFFFF	Device-nGnRnE	1

Access permission for all regions and address ranges is 0b00. Access permission 0b00 implies that the EL2 MPU Background region provides both read and write access to accesses from EL2 translation regime that hit any region in the EL2 MPU Background region.

Any accesses from EL1 that hit in EL2 MPU Background region have no read/write access and generate permission fault.

### 9.2.1.3 Default Cacheability

When default Cacheability is enabled (HCR\_EL2.DC=1), transactions using the EL1-controlled MPU Background region have Normal, Inner Write-Back, Outer Write-Back, Non-shareable attributes applied with both Read-Allocate and Write-Allocate hints enabled. Instruction accesses that hit in the Background region when HCR\_EL2.DC=1 are always executable.

The default attributes are the most permissive, meaning that when combined with any attribute from the EL2-controlled MPU the resulting attribute is the same as the EL2-controlled MPU attribute. This allows the EL2-controlled MPU to effectively make the EL1-controlled MPU transparent to transactions from the EL1 translation regime that hit in the Background region. When HCR\_EL2.DC=1, all translations from the EL0/EL1 translation regime perform a two-stage MPU lookup and the Cortex®-R82AE processor behaves as if HCR\_EL2.VM is set.

#### 9.2.1.4 Combined MPU Checking flowchart

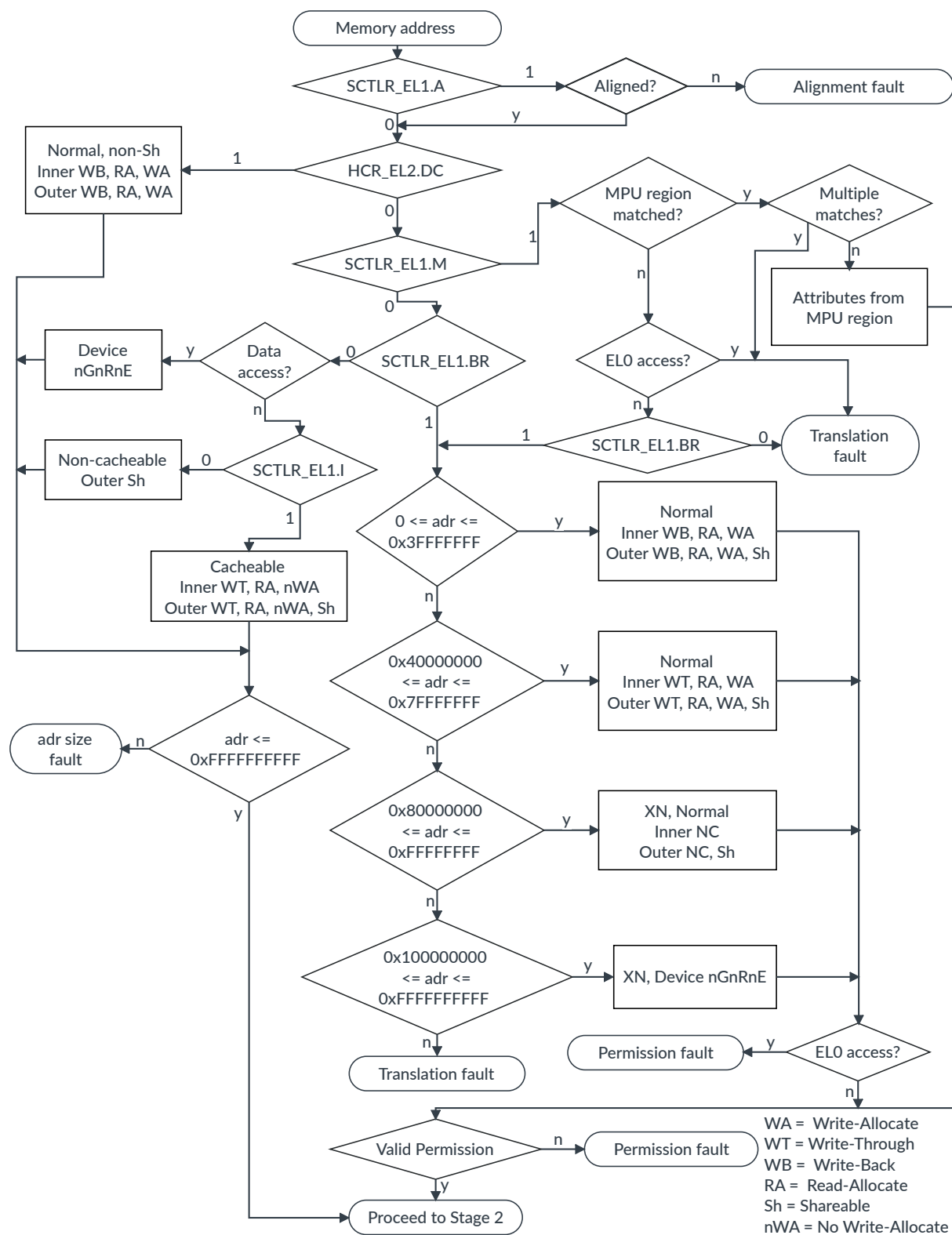
The following figure shows EL1 *Memory Protection Unit* (MPU) checking flowchart.



The figure is not exhaustive. Other System register fields might influence the Effective value of the ones mentioned on the figure, or some instructions might behave differently. For more information on the detailed description of the System register fields, see [A. AArch64 registers](#) on page 307.

---

### Figure 9-1: EL1 MPU check



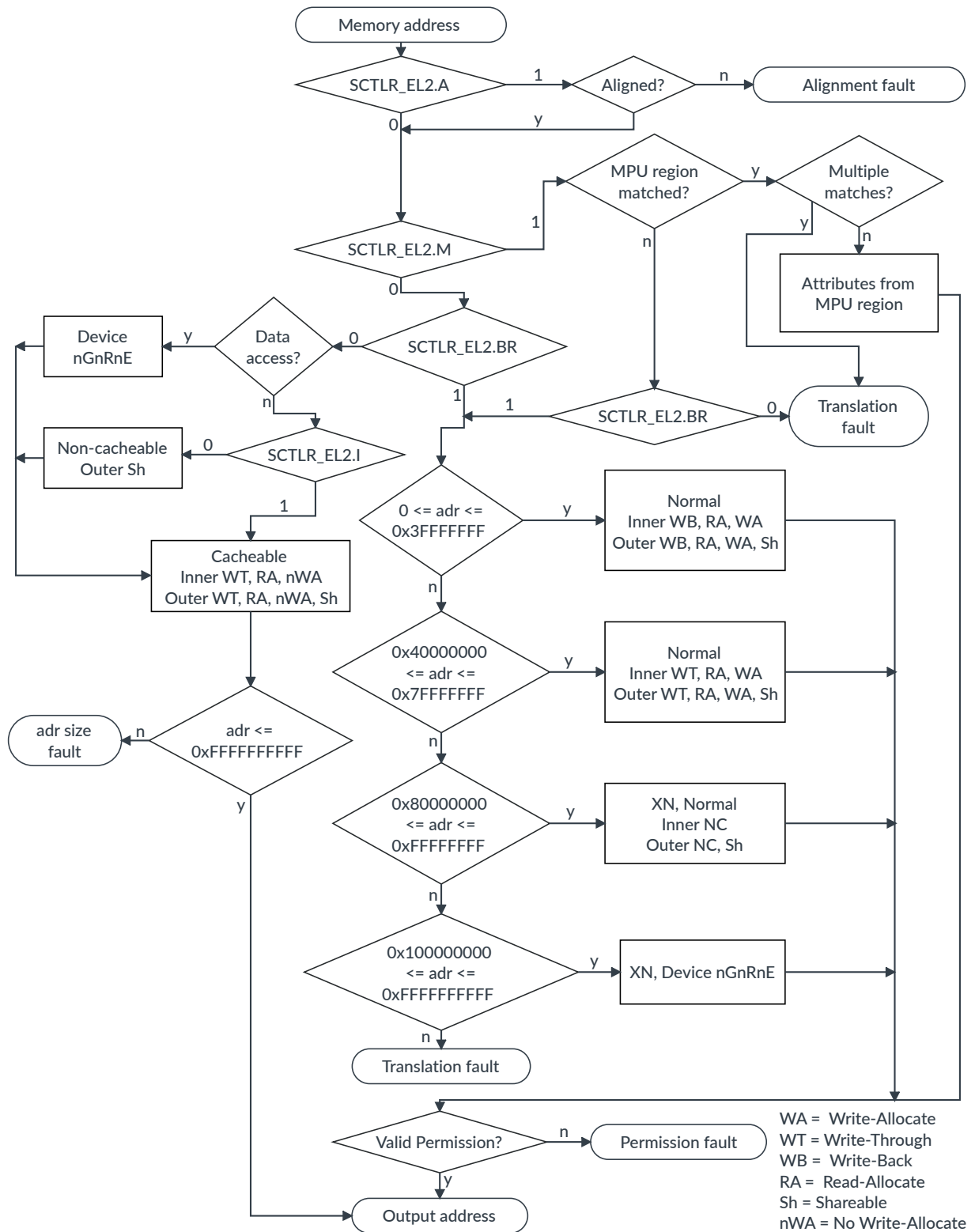
The following figure shows EL2 MPU checking flowchart.



Note

The figure is not exhaustive. Other System register fields might influence the Effective value of the ones mentioned on the figure, or some instructions might behave differently. For more information on the detailed description of the System register fields, see [A. AArch64 registers](#) on page 307.

---

**Figure 9-2: EL2 MPU check**

## 9.2.2 Virtualization support

To support virtualization, two stages of MPU lookup are performed.

Virtualization allows processes running at EL1 and EL0 (typically one or more guest operating systems and their applications) to be managed by processes running at EL2 (typically a single hypervisor).

The EL1-controlled MPU checks transactions from processes running at EL0 or EL1 and is programmed by processes running at EL1 or EL2. The EL2-controlled MPU also checks transactions executed from the EL0/EL1 translation regime when virtualization is enabled and programmed by software at EL2. Transactions executed under the EL2 translation regime use the EL2-controlled MPU only.

When virtualization is enabled (HCR\_EL2.VM=1) and the EL2-controlled MPU is enabled (SCTLR\_EL2.M=1), transactions permitted by the EL1-controlled MPU are checked by the EL2-controlled MPU as part of a two stage lookup. If both MPUs permit the transaction, memory attributes from stage 1 are combined with attributes from the matching region in stage 2 and the stricter of the two sets of attributes are applied to the transaction.

### 9.2.2.1 Combining MPU memory attributes

When a two-stage lookup is performed, the memory type, Cacheability, and Shareability attributes from each MPU are combined.

#### Combining the memory type attribute

The following table shows how the memory type assignments are combined under typical conditions as part of a two-stage lookup.

**Table 9-3: Combining the memory type assignments**

Assignment in EL1-controlled MPU	Assignment in EL2-controlled MPU	Resultant type
Device-nGnRnE	Any	Device-nGnRnE
Device-nGnRE	Device-nGnRnE	Device-nGnRnE
	Not Device-nGnRnE	Device-nGnRE
Device-nGRE	Device-nGnRnE	Device-nGnRnE
	Device-nGnRE	Device-nGnRE
	Not (Device-nGnRnE or Device-nGnRE)	Device-nGRE
Device-GRE	Device-nGnRnE	Device-nGnRnE
	Device-nGnRE	Device-nGnRE
	Device-nGRE	Device-nGRE
	Device-GRE or Normal	Device-GRE
Normal	Any type of Device	Device type assigned at stage 2
	Normal	Normal

## Force Write-Back

The attributes from the stage 1 and stage 2 translation regimes are typically combined to be the most restrictive of the two. For example, if the stage 1 translation regime returns a Device attribute and the stage 2 translation regime returns Normal memory attributes, the final combined attributes become the stricter of the two, which is Device.

However, if HCR\_EL2.FWB bit is set, the Hypervisor forces the final attributes to be Normal, Inner and Outer Write-Back when the EL2 translation regime returns Normal, Inner and Outer Write-Back. This implies that the stage 1 translation regime attributes are ignored even if they were marked as Device. This is particularly useful when the Hypervisor wants to limit the interrupt latency window by relaxing the Device attributes.



Forcing Device attribute to Normal memory allows the Cortex®-R82AE processor to make speculative accesses to peripherals, which may be undesirable.

## Combining the Cacheability attribute

The following table shows how the Cacheability assignments are combined as part of a two-stage lookup.

**Table 9-4: Combining the Cacheability assignments**

Assignment in EL1-controlled MPU	Assignment in EL2-controlled MPU	Resultant Cacheability
Non-cacheable	Any	Non-cacheable
Any	Non-cacheable	Non-cacheable
Write-Through Cacheable	Write-Through or Write-Back Cacheable	Write-Through Cacheable
Write-Through or Write-Back Cacheable	Write-Through Cacheable	Write-Through Cacheable
Write-Back Cacheable	Write-Back Cacheable	Write-Back Cacheable

## Combining the Shareability attribute

The following table shows how the Shareability assignments are combined as part of a two-stage lookup.

**Table 9-5: Combining the Shareability assignments**

Assignment in EL1-controlled MPU	Assignment in EL2-controlled MPU	Resultant Cacheability
Outer Shareable	Any	Outer Shareable
Inner Shareable	Outer Shareable	Outer Shareable
	Inner Shareable	Inner Shareable
	Non-shareable	Inner Shareable
Non-shareable	Outer Shareable	Outer Shareable
	Inner Shareable	Inner Shareable
	Non-shareable	Non-shareable



### 9.2.3 MPU register access

The MPU base and limit registers can be accessed indirectly or directly.

#### Indirectly

A region is selected by writing to the PRSEL<sub>R</sub>\_EL1 (PRSEL<sub>R</sub>\_EL2 for EL2 MPU). The selected region is programmed by writing to the PRBAR\_EL1 and PRLAR\_EL1 (PRBAR\_EL2 and PRLAR\_EL2 for EL2 MPU).

#### Directly

You can directly access only a group of 16 MPU region registers at a time by setting the PRSEL<sub>R</sub>\_EL<sub>x</sub>.REGION[7:4].

If the Cortex®-R82AE processor is implemented with 32 MPU regions, then you can directly access the first group of 16 MPU region registers from 0-15 by setting the PRSEL<sub>R</sub>\_EL<sub>x</sub>.REGION[7:4] to 0b0000. Then you can directly access the second group of 16 MPU region registers from 16-31 by setting the PRSEL<sub>R</sub>\_EL<sub>x</sub>.REGION[7:4] to 0b0001. You cannot access both groups of MPU region registers directly at the same time.

The base and limit registers for region *n*, where *n* is 0-15, are directly accessed by encoding the region number into CR<sub>m</sub> and opcode2 of the following system register access instructions:

CR<sub>m</sub> = 0b1rrr, where rrr = region\_number[3:1].

op2 = 0brr00 for PRBAR\_EL<sub>x</sub> where *r* is *n*[0] and *n* is region\_number 0-15 for the currently enabled group.

op2 = 0brr01 for PRLAR\_EL<sub>x</sub> where *r* is *n*[0] and *n* is region\_number 0-15 for the currently enabled group.

Writing base and limit registers:

```

PRBAR0_EL1 MSR PRBAR<n>_EL1, <Xt>
-
PRBAR15_EL1
PRLAR0_EL1 MSR PRLAR<n>_EL1, <Xt>
-
PRLAR15_EL1
PRBAR0_EL2 MSR PRBAR<n>_EL2, <Xt>
-
PRBAR15_EL2
PRLAR0_EL2 MSR PRLAR<n>_EL2, <Xt>
-
PRLAR15_EL2

```

Reading base and limit registers:

```

PRBAR0_EL1 MRS PRBAR<n>_EL1, <Xt>
-
PRBAR15_EL1
PRLAR0_EL1 MRS PRLAR<n>_EL1, <Xt>
-
PRLAR15_EL1
PRBAR0_EL2 MRS PRBAR<n>_EL2, <Xt>
-
PRBAR15_EL2
PRLAR0_EL2 MRS PRLAR<n>_EL2, <Xt>
-
PRLAR15_EL2

```

The Cortex®-R82AE Processor will dual issue MSR or MRS instructions accessing these registers under the following conditions:

- Both MSR or both MRS
- <N> is the same for both instructions
- Both registers are EL1 or both registers are EL2

## 9.3 MMU

The *Memory Management Unit* (MMU) is responsible for translating addresses of code and data *Virtual Addresses* (VAs) to *Physical Addresses* (PAs) in the real system. The MMU also controls memory access permissions, memory ordering, and cache policies for each region of memory.

The three main functions of the MMU are to:

- Control the table walk hardware that accesses translation tables in main memory.
- Translate *Virtual Addresses* (VAs) to *Physical Addresses* (PAs).
- Provide fine-grained memory system control through a set of virtual-to-physical address mappings and memory attributes that are held in translation tables.

Each stage of address translation uses a set of address translations and associated memory properties that are held in memory mapped tables that are called translation tables. Translation table entries can be cached into a *Translation Lookaside Buffer* (TLB).



Pagetales must be placed on the *Main Manager* (MM) port. A fault is raised if a pagewalk occurs to a different port.

---

The following table describes the MMU components.

**Table 9-6: MMU components**

Component	Description
L1 instruction TLB	15 entries, fully associative
L1 data TLB	16 entries, fully associative
L2 TLB	1024 entries, 4-way set associative
Walk cache RAM	32 entries, 4-way set associative

A TLB entry refers to the information needed to perform a translation for a single page. The TLB entries contain either one or both of a global indicator and an *Address Space Identifier* (ASID) to allow context switches without requiring the TLB to be invalidated.

The TLB entries also contain a *Virtual Machine Identifier* (VMID) to allow virtual machine switches by the hypervisor without requiring the TLB to be invalidated.



The Cortex®-R82AE processor is optimized for 16KB or larger pages. There may be a performance impact if 4KB pages are used in VMSA.

The Cortex®-R82AE processor has a physical address width that is parameterized and can be either 40 (when parameter PA\_W=40) or 48 (when parameter PA\_W=48) which allows 1TB and 256TB of physical memory, respectively, to be addressed.

### 9.3.1 TLB organization

The *Translation Lookaside Buffer* (TLB) is a cache of recently executed page translations within the *Memory Management Unit* (MMU).

The Cortex®-R82AE processor implements a two-level TLB structure. The L2 TLB stores all page sizes and is responsible for breaking these down into smaller pages when required for the data side or instruction side L1 TLB.

TLB lockdown is not supported.

After reset, an Invalidate All operation is executed and all entries in the TLB are invalidated.

#### 9.3.1.1 L1 TLB

The first level of caching for the translation table information is an L1 *Translation Lookaside Buffer* (TLB), implemented on each of the instruction and data sides.

The Cortex®-R82AE L1 instruction TLB supports 4KB pages only for a single entry.

The Cortex®-R82AE L1 data TLB supports 4KB pages only for a single entry.



L1 instruction TLB and L1 data TLB can still hold 16KB or larger pages as multiple entries. For example, an 16KB page is held as four 4KB entries. There is no performance impact with pages larger than 4KB.

Any other page sizes are fractured after the L2 TLB and the appropriate page size sent to the L1 TLB.

All TLB maintenance operations affect both the L1 instruction and data TLBs and cause them to be invalidated.

A hit in the L1 instruction TLB provides a single SCLK cycle access to the translation, and returns the PA to the instruction cache for comparison. It also checks the access permissions to signal an Instruction Abort.

A hit in the L1 data TLB provides a single SCLK cycle access to the translation, and returns the PA to the data cache for comparison. It also checks the access permissions to signal a Data Abort.

### 9.3.1.2 L2 TLB

A unified L2 *Translation Lookaside Buffer* (TLB) handles any misses from the L1 instruction and data TLBs.

The L2 TLB is a 4 way set-associative with 256 sets. Therefore it can cache up to 1024 translation results. The L2 TLB supports all *Virtual Memory System Architecture* (VMSA) block sizes, except for 1GB. See VMSAv8 in the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

A miss in the L1 data TLB or a hit in the L2 TLB has a penalty compared to a hit in the L1 data TLB. This penalty can be increased depending on the arbitration of pending requests. The best case hit penalty is 4 cycles and the worst case hit penalty is 9 cycles.

If a 1GB block is fetched, it is split into 512MB blocks and the appropriate block for the lookup is stored.

Accesses to the L2 TLB take a variable number of cycles, based on:

- Competing requests from the L1 TLBs.
- TLB maintenance operations in flight.
- Different page size mappings in use.

### 9.3.1.3 Walk cache RAM

The walk cache RAM holds the result of a stage 1 translation up to, but not including, the last level.

### 9.3.2 TLB match process

The Arm®v8-R AArch64 architecture provides support for multiple *Virtual Address* (VA) spaces that are translated differently.

*Translation Lookaside Buffer* (TLB) entries store the context information that is required to facilitate a match and avoid the need for a TLB flush on a context or virtual machine switch.

Each TLB entry contains a:

- VA.
- *Physical Address* (PA).
- Set of memory properties that includes type and access permissions.

Each entry is either associated with a particular *Address Space Identifier* (ASID) or is global. In addition, each TLB entry contains a field to store the *Virtual Machine Identifier* (VMID) in the entry applicable to accesses from Non-secure EL0 and EL1 Exception levels.

Each TLB entry is associated with a particular translation regime:

- EL0 or EL1 in Secure state

A TLB match entry occurs when the following conditions are met:

- When VA[48:N] matches the requested address, where N is  $\log_2$  of the block size for that translation that is stored in the TLB entry, moderated by the page size.
- The ASID matches the current ASID held in the CONTEXTIDR, TTBR0, or TTBR1 register, or the entry is marked global.
- The VMID matches the current VMID held in the VTTBR\_EL2 register.

### 9.3.3 Translation table walks

When an access to an address is requested, the *Memory Management Unit* (MMU) searches for the requested *Virtual Address* (VA) in the *Translation Lookaside Buffers* (TLBs). If it is not present, then it is a miss and the translation proceeds by looking up the translation table during a translation table walk.

When the Cortex®-R82AE processor generates a memory access, the MMU:

1. Performs a lookup for the requested VA and current translation regime in the relevant instruction or data L1 TLB.
2. If there is a miss in the relevant L1 TLB, the MMU performs a lookup for the requested VA, current ASID, current VMID, and translation regime in the L2 TLB.
3. If there is a miss in the L2 TLB, the MMU performs a hardware translation table walk.

In the case of an L2 TLB miss, the hardware does a translation table walk as long as the MMU is enabled and the translation using the base register has not been disabled.

If the translation table walk is disabled for a particular base register, the Cortex®-R82AE processor returns a translation fault.

If the TLB finds a matching entry, it checks the access permission bits and the domain to determine if the access is permitted. If the matching entry does not pass the permission checks, the MMU signals a permission fault.

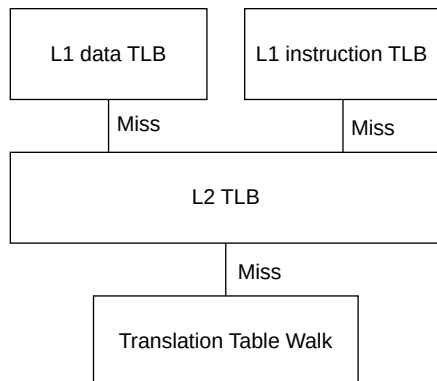
See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for details of Permission faults, including:

- A description of the various faults
- The fault codes.
- Information regarding the registers where the fault codes are set.

In translation table walks the descriptor is fetched from the L2 memory system.

The following figure shows the translation table walk process:

**Figure 9-3: Translation table walks**



### 9.3.4 MMU memory accesses

During a translation table walk, the *Memory Management Unit* (MMU) generates accesses. This section describes the specific behaviors of the Cortex®-R82AE processor for MMU memory accesses.

### 9.3.4.1 Configuring MMU accesses

Translation table walk can be performed in Cacheable or Non-cacheable regions. This is determined by the translation table walk memory attributes, which can be affected by several different configurations:

- IRGN and ORGN bits in the TCR\_EL1 registers which define the memory type for translation table walk.
- SCTLR\_ELx.C and HCR\_EL2.CD which affect the table walk to Cacheable or Non-cacheable memory.
- Stage 2 memory attributes for stage 1 translation table walk, which affect the stage 1 translation table walk memory attribute.

Only when the final translation table walk memory attribute is Inner Write-Back and Outer Write-Back and the cache is enabled, the translation table walk accesses the cacheable memory.

For more information on the control fields, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

### 9.3.4.2 Hardware management of the Access flag

The Cortex®-R82AE processor includes the option to perform hardware updates to the translation tables.

This feature is enabled in register TCR\_EL1.

The Cortex®-R82AE processor supports hardware updates to the Access flag only when the translation tables are held in Inner Write-Back and Outer Write-Back Normal memory regions. The Cortex®-R82AE processor does not support hardware management of dirty state.

If software requests a hardware update in a region that is not Inner Write-Back or Outer Write-Back Normal memory, then the Cortex®-R82AE processor returns an abort with the following encoding:

- ESR\_ELx.DFSC = 0b110001 for Data Aborts.
- ESR\_ELx.IFSC = 0b110001 for Instruction Aborts.

For more information about hardware updates of the Access flag, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

## 9.3.5 Responses

Certain faults and aborts can cause an exception to be taken because of a memory access.

### 9.3.5.1 MMU responses

When one of the following translations is completed, the *Memory Management Unit* (MMU) generates a response to the requester:

- An L1 instruction or L1 data *Translation Lookaside Buffer* (TLB) hit.
- An L2 TLB hit.
- A translation table walk.

The response from the MMU contains the following information:

- The *Physical Address* (PA) corresponding to the translation.
- A set of permissions.
- Secure or Non-secure state information.



The Secure or Non-secure state information is the security state of the descriptor and not the security state of the Cortex®-R82AE processor. The Cortex®-R82AE processor always operates in Secure state but can access both Secure and Non-secure physical memory address space.

---

- All the information that is required to report aborts.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more details.

### 9.3.5.2 MMU aborts

The *Memory Management Unit* (MMU) can detect faults that are related to address translation and can cause exceptions to be taken to the individual core within the Cortex®-R82AE processor.

Faults can include address size, translation, access flags, and permissions. See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information about aborts.

### 9.3.5.3 External aborts

External aborts are aborts that occur in the memory system that are different than the *Memory Management Unit* (MMU) detects. External aborts are caused by errors flagged by the external memory interfaces or are generated because of an uncorrected ECC error in the L1 data cache or L2 cache arrays.

When an External abort to the external interface occurs on a translation table walk access, the MMU returns a synchronous External abort. For a Load pair or a Store pair operation, the address captured in the fault register is that of the address that generated the synchronous external abort.



### 9.3.5.4 Misprogramming contiguous hints

A programmer might misprogram the translation tables so that:

- The block size being used to translate the address is larger than the size of the input address.
- The address range translated by a set of blocks that is marked as contiguous, by use of the contiguous bit, is larger than the size of the input address.

If there is this kind of misprogramming, the Cortex®-R82AE processor does not generate a translation fault.

### 9.3.5.5 Conflict aborts

Conflict aborts are generated from the L1 instruction or data *Translation Lookaside Buffer* (TLB). If a conflict abort is detected in the L2 TLB, it chooses one valid translation. The L2 TLB does not generate a conflict abort.

## 9.3.6 Memory behavior and supported memory types

The Cortex®-R82AE processor support all the Arm®v8-R AArch64 memory types.

These device memory types have the following three attributes:

#### **G – Gathering**

The capability to gather and merge requests together into a single transaction.

#### **R – Reordering**

The capability to reorder transactions.

#### **E – Early Write Acknowledgement**

The capability to accept early acknowledge of transactions from the interconnect.

The permitted combinations are described in the following table:

**Table 9-7: Supported Arm®v8-R AArch64 Device memory types**

Memory type	Description
Device-GRE	Device Gathering, Reordering, Early Write Acknowledgement.  Device-GRE is similar to Normal Non-cacheable but does not permit Speculative accesses.
Device-nGRE	Device non-Gathering, Reordering, Early Write Acknowledgement.  Transactions might be reordered within the L2 memory system or in the system interconnect.  The use of barriers is required to order accesses to Device-nGRE memory.

Memory type	Description
Device-nGnRE	Device non-Gathering, non-Reordering, Early Write Acknowledgement.  Device-nGnRE is equivalent to the Device memory type in earlier versions of the architecture.  Device-nGnRE is treated the same as nGnRnE inside the Cortex®-R82AE processor but is reported differently on the bus interface.
Device-nGnRnE	Device non-Gathering, non-Reordering, No Early Write Acknowledgement.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information.

Write-Through and Mixed inner and outer Cacheability not included.

### 9.3.7 Page-based hardware attributes

*Page-Based Hardware Attributes* (PBHA) is not supported by the Cortex®-R82AE processor.

## 10. RAS Extension support

This chapter describes the *Reliability, Availability, and Serviceability* (RAS) features implemented in the Cortex®-R82AE processor.

### 10.1 RAS Extension support in the processor

The Cortex®-R82AE processor reports and records errors in memories and system ports according to the *Reliability, Availability, and Serviceability* (RAS) Extension for the Arm®v8.4 architecture.



Errors detected on speculative accesses are recorded but no exceptions (synchronous or asynchronous) are generated. If the Cortex®-R82AE processor attempts to consume a poisoned location later, an exception will be taken at that time.

The RAS Extension and RAM protection are always present in the Cortex®-R82AE processor, however several safety mechanisms are optional. The error types that can be reported via RAS are dependent on the specific configuration and system in which the Cortex®-R82AE processor is integrated. This chapter will describe all errors that can be detected and reported via RAS.

In particular, the Cortex®-R82AE processor RAS implementation supports capturing errors from the following safety mechanisms:

- Cache protection with *Single Error Correct Double Error Detect* (SECCDED) on the RAMs that contain dirty data or coherency state. This includes the *Instruction Tightly Coupled Memory* (ITCM), *Data Tightly Coupled Memory* (DTCM), RAMs, L1 data cache data and dirty RAMs, L2 cache tag and data RAMs, L2 cache data buffers, L2 duplicate L1 tag RAMs, and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs.
- Cache protection with *Double Error Detect* (DED) on the RAMs that only contain clean data or, in the case of the L1 data cache tag RAM, data that can be corrected via the duplicate L1 tag RAMs. This includes the L1 instruction cache tag and data RAMs, L1 data cache tag RAM, and the *L2 Translation Lookaside Buffer* (TLB) tag and data RAMs.
- Non-ECC related memory errors resulting in loss of dirty or poison state due to external error responses and/or misconfiguration.
- Optional Bus Protection for all external interfaces, excluding interfaces which are not active in mission mode such as debug and trace. This is implemented via AMBA interface protection standards where possible, and odd parity otherwise.
- A Bus Timeout detection mechanism for all AMBA manager interfaces capable of detecting when responses are not received within a programmable time limit.
- An interrupt monitor capable of detecting when interrupts are masked for longer than a programmable time limit, or a core is pending in WFX without receiving an event or interrupt for longer than a programmable time limit.

- A Livelock Detector, capable of detecting when a single exception has been repeatedly taken, preventing forward progress.
- Optional Transient Fault Protection (“Flop Parity”) which protects all registers in the core with odd parity.

Note, the L2 Cache replacement RAMs and the branch predictor RAMs are out of the scope of RAS, as errors in these RAMs cannot cause a functional issue, impacting only performance. The Cortex®-R82AE processor remains robust in the presence of any errors in these RAMs. Note that any concerns around errors impacting performance can be monitored via a watchdog timeout.

The Cortex®-R82AE RAS implementation also supports the following key features:

- The *Error Synchronization Barrier* (ESB) instruction. When an ESB instruction is executed, the core ensures that all unrecoverable SError Interrupts that are generated by instructions before the ESB are either taken by the core or pended in DISR\_EL1.
- The implicit ESB instruction as described in the [Arm® Architecture Reference Manual Supplement Reliability, Availability, and Serviceability \(RAS\), for A-profile architecture](#).
- Support for poison on cache allocations and external bus accesses, allowing for detected errors to be deferred until they are consumed.
- *Fault Handling Interrupts* (FHIs).
- *Error Recovery Interrupts* (ERIs).
- *Critical Error Interrupt* (CEI).
- Error injection.

The Cortex®-R82AE processor has five RAS nodes, Node 0, Node 1, and Node 4, Node 7 and Node 8, containing a total of nine Error Records:

- Node 0 for shared memory non-ECC errors from the L2 cache and LCU. This node corresponds to Error Record register 0.
- Node 1 for per-core memory errors from the L1 data cache, L1 instruction cache, *Tightly Coupled Memories* (TCMs) (ITCM and DTCM), and the L2 TLB RAMs. This node corresponds to Error Record registers 1-3.
- Node 4 for shared memory errors from the L2 cache data RAMs, L2 cache tag RAMs, L2 cache data buffer RAMs, L2 cache duplicate L1 tag RAMs, and the LCU duplicate L1 tag RAMs. This node corresponds to Error Record registers 4-6.
- Node 7 for per-core bus errors from the *Low-latency Peripheral Port* (LLPP) as well as errors detected via the livelock detector and flop parity. Node 7 corresponds to Error Record register 6.
- Node 8 for shared bus errors from the *Main Manager* (MM), *Low-latency RAM* (LLRAM), *Shared Peripheral Port* (SPP), *ACE-Lite Subordinate* (ACELS), *Main Accelerator Coherency Port* (MACP), GIC interface, and Utility bus as well as errors from the interrupt monitor. Node 8 corresponds to Error Record register 7.

If bus protection is configured, then the Cortex®-R82AE processor has additional two RAS nodes, Node 7 and Node 8 and two Error Record registers, Error Record registers 7 and 8, implemented:

- Node 7 for per-core bus errors from the *Low-latency Peripheral Port* (LLPP). Node 7 corresponds to Error Record register 6.
- Node 8 for shared bus errors from the *Main Manager* (MM), *Low-latency RAM* (LLRAM), *Shared Peripheral Port* (SPP), *ACE-Lite Subordinate* (ACELS), *Main Accelerator Coherency Port* (MACP), GIC interface, and Utility bus. Node 8 corresponds to Error Record register 7.

The following table shows per-core and shared nodes and error record registers in the Cortex®-R82AE processor.

**Table 10-1: RAS nodes and error record registers**

Node	Error Record register	Error types recorded	Usage	RAS node control
0	0	Non-ECC memory errors from L2 cache and LCU	Shared	ERR0CTLR
1	1, 2, 3	Memory errors from L1 Instruction Cache, L1 Data Cache, ITCM, DTCM and L2 TLB	Per-core	ERR1CTLR
4	4, 5, 6	Memory errors from L2 cache and LCU	Shared	ERR4CTLR
7	7	Other safety mechanism error for the core	Per-core	ERR7CTLR
8	8	Other safety mechanism error for the cluster	Shared	ERR8CTLR

For more information on the architectural RAS Extension and the definition of a RAS node, see the [Arm® Architecture Reference Manual Supplement Reliability, Availability, and Serviceability \(RAS\), for A-profile architecture](#).

## 10.2 Memory protection behavior

The Cortex®-R82AE processor is robust in the presence of 1-bit or 2-bit errors in any of its RAMs.

The Cortex®-R82AE processor employs a variety of error detection and correction schemes. *Single Error Correct Double Error Detect* (SECCDED) *Error Correcting Code* (ECC) is used if there is a need to produce corrected data from the error data. *Double Error Detect* (DED) ECC is used when error detection is sufficient and the corrected data is obtained from a different processor memory. Cortex®-R82AE also makes use of non-RAM redundancy or functional correctness by construction to protect from 1-bit and 2-bit errors in the branch predictor and L2 replacement RAMs. For example, errors in the branch predictor RAMs cannot cause a functional issue - a mispredicted branch as a result of an error will be resolved and the pipeline will be flushed and the correct instruction fetched. 1-bit and 2-bit errors are corrected automatically by design. Equally the L2 replacement RAM is used to improve cache eviction policy; errors will only result in a different victim being selected and execution will continue as normal.

In the Cortex®-R82AE SECCDED and DED schemes, when the datum and code bits are all-zero, or all-one, the interpretation is that an error has occurred that the ECC scheme cannot correct. When the datum and code bits are both located within a single physical RAM instance, RAM failure

modes that results in all-zero or all-one output will be detected as a fatal error. However in some cases it may still be possible to correct, such as when the data is known to be clean and can be invalidated and refetched.

When the datum and code bits are both located within a single physical RAM instance, RAM failure modes that results in all-zero or all-one output will be detected as a fatal error.

Regardless of the state of the processor, the Cortex®-R82AE processor records the error at the point when it is detected.

When the Cortex®-R82AE processor is operating in Lock or Hybrid mode, the primary cluster or core level memories are used to provide responses to the redundant cores. This improves availability by ensuring that error detection and correction apply to the lockstep pair.

The following table indicates which protection type is applied to each RAM. The ECC granule specifies how much data is used to compute a single ECC code.

**Table 10-2: RAM protection**

RAMs	Protection scheme	Error type	Action
Instruction Tightly Coupled Memory (ITCM)	SECDED 64 bits	1-bit	Correct the error
		2-bit	Poison RAM location
Data Tightly Coupled Memory (DTCM)	SECDED 32 bits	1-bit	Correct the error
		2-bit	Poison RAM location
L1 instruction cache data	DED 64 bits	1-bit/2-bit	Evict cache line and refetch clean line from L2 cache, LLRAM, or MM
L1 instruction cache tag	DED 30 bits <sup>1</sup>	1-bit/2-bit	Evict cache line and refetch clean line from L2 cache, LLRAM, or MM
L1 data cache data	SECDED 32 bits	1-bit	Evict cache line, correcting the error when needed, and refetch clean line from L2 cache, LLRAM, or MM.
		2-bit	Poison the location or evict poison to the L2
L1 data cache tag	DED Up to 31 bits <sup>2</sup>	1-bit/2-bit	Evict cache line and refetch clean line, retrieving correct tags from the L2/LCU duplicate L1 tag memories
L1 data cache dirty	SECDED 2 bits	1-bit	Correct the error
		2-bit	Assume cache line is clean, dirty data discarded
L2 cache data	SECDED 128 bits	1-bit	Correct the error
		2-bit	Poison the location

<sup>1</sup> Granule size is configuration dependent.

<sup>2</sup> Granule size is configuration dependent.

RAMs	Protection scheme	Error type	Action
L2 cache tag	SECDED Up to 33 bits <sup>3</sup>	1-bit	Correct the error
		2-bit	The L2 Cache provides the IMP_CLUSTERACTLR_EL1.L2ECHLT software control that enables additional error containment support in the event of detecting an uncontainable error in the L2 Cache or L2 Duplicate L1 tags. When enabled, a fatal error in the tag RAMs will prevent the instruction from being replayed and instead stall all subsequent coherent accesses to the L2 Cache and L2 Duplicate L1 Tag RAMs. This will still cause failure of the affected execution thread(s), but it will prevent the consumption of corrupt state without any error indication. The stall behavior will remain until reset of the L2. Note that if the L2 is configured with L2_SLICES=2 each L2 slice will be stalled independently as the RAMs are split between the two slices. MBIST requests will still be allowed to access the RAMs when the L2 has entered this stall condition.
L2 cache data buffers	SECDED 144 bits	1-bit	Correct the error
		2-bit	Poison the location
L2 duplicate L1 tag	SECDED Up to 32 bits <sup>4</sup>	1-bit	Correct the error
		2-bit	Evict cache line and refetch clean line from MM, unless location is about to be overwritten, or optionally stall the request
LLRAM Coherency Unit (LCU) duplicate L1 tag	SECDED Up to 18 bits <sup>5</sup>	1-bit	Correct the error
		2-bit	Evict cache line and refetch clean line from LLRAM
L2 cache replacement	Functional correctness by construction	1-bit/2-bit	Cache evicts a line that might be different compared with the replacement policy. No error results from selecting a different line. Errant entry replaced with correct data.
Branch predictor	Non-RAM redundancy	1-bit/2-bit	Error data checked and corrected by core pipeline
L2 Translation Lookaside Buffer (TLB) data	DED 46 bits	1-bit/2-bit	Discard the translation and repeat the page walk
L2 TLB tag	DED 68 bits	1-bit/2-bit	Discard the translation and repeat the page walk

## Error correction

The Cortex®-R82AE processor corrects all single bit errors either by correcting the error (inline correction for caches and TCMs, or overwriting with correct data for branch predictors and L2 cache replacement) or by evicting the related cache line and by re-fetching a clean copy from a different memory. Therefore, single bit errors do not affect the function of the Cortex®-R82AE processor, although they might affect timing. If there are multiple single bit errors in different RAMs, or in different protection granules in the same RAM, then the Cortex®-R82AE processor also remains functionally correct.

<sup>3</sup> Granule size is configuration dependent.

<sup>4</sup> Granule size is configuration dependent.

<sup>5</sup> Granule size is configuration dependent.

If there is a double bit error in a single RAM in a single protection granule, then the Cortex®-R82AE processor detects the error. If the data can be found in a different memory (such as the clean data in a cache) or can be recomputed (such as branch outcomes or L2 cache replacement), the Cortex®-R82AE processor attempts to correct the error by evicting the cache line and by re-fetching a clean copy from a different memory. If the data cannot be found elsewhere (such as the TCM data or dirty data in a cache), then the data is lost. In some cases, such as a double bit error on a tag RAM of a dirty cache line, the coherency state might be lost, for example because:

- The address of the erroneous cache line has become **UNKNOWN** and the location cannot be poisoned, or
- The coherent state of the line has been lost and it is no longer possible to determine if a line is clean or dirty.

In addition to correcting the data read from protected RAMs, the Cortex®-R82AE processor also either writes the corrected data back into the protected RAMs or it invalidates the erroneous location or poisons the erroneous location. This allows it to avoid the accumulation of errors that leads to correctable errors combining into uncorrectable errors or double bit errors combining into triple bit errors.

If there are three or more bit errors in the same protection granule, then depending on the RAM and the position of the errors in the RAM, the Cortex®-R82AE processor might or might not detect the errors.

The memory protection feature of the Cortex®-R82AE processor has a minimal performance impact when no errors are present.

The Cortex®-R82AE processor also includes hard error handling mechanisms to guarantee forward progress in the presence of a limited number of hard correctable errors. A hard error is a physical error in the RAM that prevents the correct value being written, for example, due to a permanently stuck-at bitcell.

A single hard error can be corrected and is guaranteed to make progress. However, if there are multiple hard errors then in some cases this can cause live-locks as the line could continuously replay.

The following table describes the hard error avoidance mechanisms for the Cortex®-R82AE RAMs.

**Table 10-3: RAM hard error avoidance mechanisms**

RAMs	Mechanism
<i>Instruction Tightly Coupled Memory</i> (ITCM)	Single 128-bit correction buffer acts as Write-Through cache
<i>Data Tightly Coupled Memory</i> (DTCM)	Single 128-bit correction buffer acts as Write-Through cache
L1 instruction cache data	Cache line has been invalidated; replayed access treated as Non-cacheable
L1 instruction cache tag	Cache line has been invalidated; replayed access treated as Non-cacheable
L1 data cache data	<i>Cache Line Avoidance Register</i> (CLAR) to mask hits and allocations on most recently affected cache line
L1 data cache tag	CLAR to mask hits and allocations on most recently affected cache line
L1 data cache dirty	CLAR to mask hits and allocations on most recently affected cache line



RAMs	Mechanism
L2 cache data	Correct inline to allow current request to proceed
L2 cache tag	Replayed access streams from the tag write buffer to avoid the cache RAM
L2 cache data buffers	Correct inline to allow current request to proceed
L2 cache replacement RAMs	Request proceeds by evicting a cache line that might be different compared with the replacement policy
L2 duplicate L1 tag	Replayed access streams from the tag write buffer to avoid the RAM
LLRAM Coherency Unit (LCU) duplicate L1 tag	Correct in-line or invalidate and allow current request to proceed
Branch predictor	Execution proceeds from the correct branch target
L2 Translation Lookaside Buffer (TLB) data	CLAR to mask affected data
L2 TLB tag	CLAR to mask affected data

The CLAR is a dedicated structure that caches the most recently corrected error. Future requests to the same location use the CLAR contents instead of reading again from the affected RAM.

## 10.3 Bus protection behavior

The Cortex®-R82AE processor can be configured with bus protection (`BUS_PROTECTION = 1`) that follows the AMBA® interface protocol.

If the Cortex®-R82AE processor is configured with bus protection, then an additional RAS two nodes are implemented and error record registers 6 and 7 become available. As a result, any bus error is recorded in the corresponding error record register in addition to raising an exception.

The following table shows the Cortex®-R82AE processor ports and the protection type.

**Table 10-4: Bus protection**

Bus	Interface type	Bus protection
Main Manager (MM) when configured as AXI	AXI5	Check_Type = Odd_Parity_Byte_All
Main Manager (MM) when configured as CHI	CHI.E	Check_Type = Odd_Parity_Byte_All
Low-latency RAM (LLRAM)	AXI5	Check_Type = Odd_Parity_Byte_All
Main Accelerator Coherency Port (MACP)	ACE5-Lite	Check_Type = Odd_Parity_Byte_All
ACE-Lite Subordinate (ACELS)	ACE5-Lite	Check_Type = Odd_Parity_Byte_All
Shared Peripheral Port (SPP)	AXI5	Check_Type = Odd_Parity_Byte_All
Low-latency Peripheral Port (LLPP)	AXI5	Check_Type = Odd_Parity_Byte_All
Utility bus	AXI5	Check_Type = Odd_Parity_Byte_All
Generic Interrupt Controller (GIC)	AXI5-Stream	Check_Type = Odd_Parity_Byte_All
Debug	APB5	Check_Type = Odd_Parity_Byte_All
Trace	ATB4	Not protected.
Embedded Logic Analyzer (ELA)	ATB4	Not protected.
P Channels	P-Channel	Not protected.
Q Channels	Q-Channel	Not protected.

## 10.4 Error Containment

The Cortex®-R82AE processor supports error containment which makes sure that an error is detected and not silently propagated wherever possible.

Error containment also implies support for poisoning to ensure that errors are reported only when the erroneous data is consumed, and the erroneous state is not lost as the data propagates throughout the cache hierarchy.

Support for the *Implicit Error Synchronization Barrier* (IESB) also allows further isolation of imprecise exceptions and future operations that are reported when poisoned data is consumed.



Using IESB might affect your interrupt latency response. For more information on interrupt latency, see [8.15.1 Interrupt latency](#) on page 204.

The Cortex®-R82AE processor avoids Uncontainable errors wherever possible, with the following exceptions for each RAS node.

Uncontainable errors can lead to UNPREDICTABLE behavior. They can result in further data corruption, or in software algorithms deadlocking as they can read inconsistent data. It is generally not possible to cleanly recover from such errors. The Cortex®-R82AE processor will generate the critical error interrupt, nCOMPLEXCRITIRQ, in the presence of Uncontainable errors if the Critical Error Interrupt is enabled. Arm recommends that in response to nCOMPLEXCRITIRQ interrupts a system reset is performed as soon as possible.

In some cases, it is possible for an error to be counted more than once. For example, multiple accesses might read the location with the error before the line is evicted.

### 10.4.1 Node 0: Non-ECC Memory Errors

The following uncontainable errors can occur at Node 0.

- If a poisoned cache line is evicted or snooped from the cluster and the interconnect does not support poisoning the Cortex®-R82AE processor reports an Uncontainable error to this RAS node before transferring the data, since the poison state is lost. Software can indicate if the interconnect supports poisoning or not by setting the interconnect data poisoning bit in the cluster control register.
- If an uncorrectable error is transferred from the L2 Cache Data Buffers (L2DBs) to the MM port and the interconnect does not support poisoning the Cortex®-R82AE processor reports an Uncontainable error to this RAS node before transferring the data, since the poison state is lost. Software can indicate if the interconnect supports poisoning or not by setting the interconnect data poisoning bit in the cluster control register.
- If a data error response is received for a MM request when configured for CHI, with the response including the PassDirty attribute but ECC checking disabled, the Cortex®-R82AE

processor reports an Uncontainable error to this RAS node. The dirty data cannot be poisoned and the poison state is lost.

- If a poisoned line is received from the MM or LLRAM but ECC checking is disabled, the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. The poison state is lost.
- If an eviction of a MM line from the L1 D-Cache or L2 Cache receives a non-data error response (SLVERR or DECERR when configured for AXI, or NDERR when configured for CHI) the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. It is unknown if the line is successfully written to memory, potentially resulting in a loss of coherency for the line.

### 10.4.2 Node 1: Core Memory Errors

The following uncontainable errors can occur at Node 1.

- If a fatal double bit error is detected on the L1 data cache dirty RAM the processor reports an Uncontainable error to this RAS node. When a snoop detects a fatal dirty RAM error, it cannot determine whether the line is clean or dirty. The data is assumed to be clean since the coherent state is unknown, and therefore might not drain data to the L2 cache and the data may be lost.

### 10.4.3 Node 4: Cluster Memory Errors

The following uncontainable errors can occur at Node 4.

- If a fatal double bit error is detected on the L2 cache tag RAM the processor reports an Uncontainable error to this RAS node. The hit/miss status and address associated with the cache line is unknown. To proceed, the line is invalidated in the L2 cache and the access is replayed and coherent state may be lost. Optionally, Cortex®-R82AE can instead be configured to halt accesses to the L2 in the presence of a fatal double bit error on the L2 cache tag RAM. This can be used to contain this error as no invalidation occurs, but forward progress on the MM interface is no longer possible. This might be used to facilitate fault handling intervention without the error having silently propagated throughout the coherency domain.
- If a fatal double bit error is detected on the L2 duplicate L1 tag RAM the processor reports an Uncontainable error to this RAS node. This hit/miss status and address associated with the cache line is unknown. To proceed, the line is invalidated in both the L2 duplicate L1 tag RAM and the corresponding L1 cache and the access is replayed and coherent state may be lost. Optionally, Cortex®-R82AE can instead be configured to halt accesses to the L2 in the presence of a fatal double bit error on the L2 cache duplicate L1 tag RAM. This can be used to contain this error as no invalidation occurs, but forward progress on the MM interface is no longer possible. This might be used to facilitate fault handling intervention without the error having silently propagated throughout the coherency domain.
- The Cortex®-R82AE processor supports an error containment feature for Node 4 which converts all uncontainable errors into unrecoverable by stalling the L2 memory system instead of invalidating and silently propagating the error. This option can be used to prevent the error propagating throughout the coherency domain, but will prevent forward progress of the L2 memory subsystem. This option can be enabled via IMP\_CLUSTERACTLR\_EL1.L2EC.

### 10.4.4 Node 7: Core Safety Mechanism Errors

The following uncontainable errors can occur at Node 7.

- When configured with bus protection, if an LLPP bus protection error is detected on an external interface, except where the error is associated with a data payload, the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. Bus protection uses odd parity protection, therefore it is not possible to know if the primary signal or the parity signal is at fault. Forward progress is not guaranteed and processor state may be corrupted. Note, data payloads are excluded as corrupt data can be poisoned, resulting in a Deferred error.
- If an LLPP bus timeout error occurs the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. While no information is lost, a timeout condition implies that forward progress is not guaranteed and the interface may be deadlocked. If configured with aborts enabled the timeout mechanism will prevent subsequent accesses to the interface and trigger an exception.
- If the livelock detector observes the exact same exception being taken 10 times without any other instructions retiring the Cortex®-R82AE processor will report an Uncontainable error to this RAS node. Forward progress is not guaranteed.
- If configured with Flop Parity and an error is detected the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. It is unknown whether the primary or parity registers are corrupt. Forward progress is not guaranteed and the processor state may be corrupted.

### 10.4.5 Node 8: Cluster Safety Mechanism Errors

The following uncontainable errors can occur at Node 8.

- When configured with bus protection, if a non-LLPP bus protection error is detected on an external interface, except where the error is associated with a data payload, the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. Bus protection uses odd parity protection, therefore it is not possible to know if the primary signal or the parity signal is at fault. Forward progress is not guaranteed and processor state may be corrupted. Note, data payloads are excluded as corrupt data can be poisoned, resulting in a Deferred error.
- If a MM, LLRAM or SPP bus timeout error occurs the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. While no information is lost, a timeout condition implies that forward progress is not guaranteed and the interface may be deadlocked. If configured with aborts enabled the timeout mechanism will prevent subsequent accesses to the interface and trigger an exception.
- If the interrupt monitor detects an error (either WFX pending for more than the programmed timeout, or interrupt masked for more than the programmed timeout) the Cortex®-R82AE processor reports an Uncontainable error to this RAS node. While no information is lost, a timeout condition implies that forward progress is not guaranteed and the core may be deadlocked.

## 10.4.6 Non-RAS Errors

The following non-RAS uncontainable errors can occur.

- If an uncorrectable error is detected in the L2DBs then the byte strobes associated with the write may be lost. The poisoned write propagated on the external interface in this scenario may access bytes not written by the original request in cases where a partial poison granule is being written. This may result in clean data getting poisoned for those incorrectly accessed byte lanes. This is not reported as an Uncontainable error within the Cortex®-R82AE processor as no information has been lost, however this error might have system implications.
- SError exceptions taken by the core due to an asynchronous error in the memory system also trigger an uncontainable error, however this is not reported to RAS (if this was a result of an ECC error the appropriate RAS event will occur, but this could also be a result of external error responses). Instead, the exception syndrome will indicate the severity of the error. In this case the exception is likely to be taken by the core after the instruction which triggered it has already retired, and therefore subsequent instructions may have been able to proceed based on corrupt architectural state.

## 10.5 Fault detection and reporting

When the Cortex®-R82AE processor detects a fault, it raises a *Fault Handling Interrupt* (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors.

### 10.5.1 Fault Handling Interrupts

When the Cortex®-R82AE processor detects a fault, it raises a *Fault Handling Interrupt* (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors.

When the Cortex®-R82AE processor detects a fault, it raises a **FAULT HANDLING INTERRUPT** (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors. nCOREERRIRQ indicates a per-core RAS node (1, 7) has been updated while nCOMPLEXERRIRQ indicates a cluster RAS node (0, 4, 8) has been updated.

When ERR<n>CTLR.FI is set, all detected Deferred errors and Uncorrected errors that the RAS node detects raise a **FAULT HANDLING INTERRUPT** (FHI).

When ERR<n>CTLR.CFI or any other CE-counter overflow bits are set, then all detected Corrected errors also generate a core or cluster FHI respectively.

## 10.5.2 Error Recovery Interrupts

When the Cortex®-R82AE processor detects a fault, it raises a *Fault Handling Interrupt* (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors.

When the RAS node is configured to do so, the Cortex®-R82AE processor raises an Error Recovery Interrupt exception through the fault signals. nCOREFAULTIRQ indicates a per-core RAS node (1,7) has been updated while nCOMPLEXFAULTIRQ indicates a cluster RAS node (0, 4, 8) has been updated.

When ERR<n>CTLR.UI is set, all detected Uncorrected errors that are not deferred generate an error recovery interrupt.

## 10.5.3 Critical Error Interrupts

When the Cortex®-R82AE processor detects a fault, it raises a *Fault Handling Interrupt* (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors.

When ERR<n>CTLR.CI is set, all Uncontainable errors that the Cortex®-R82AE processor detects generate a critical error interrupt on the nCOMPLEXCRITIRQ signal.

## 10.5.4 Clearing reported faults

When the Cortex®-R82AE processor detects a fault, it raises a *Fault Handling Interrupt* (FHI) exception through the fault signals. FHIs are reflected in the Error Record registers that are updated in the node that detects the errors.

The nCOREFAULTIRQ, nCOREERRIRQ, nCOMPLEXFAULTIRQ, nCOMPLEXERRIRQ, and nCOMPLEXCRITIRQ signals remain asserted until software clears them by writing the ERR<n>STATUS register.

Arm recommends that at least the nCOMPLEXERRIRQ, nCOMPLEXCRITIRQ, and nCOREERRIRQ pins are connected to the interrupt controller, so that an interrupt or system error is generated when the pin is asserted.

## 10.6 Exceptions

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

The Cortex®-R82AE processor might raise:

- A **SYNCHRONOUS EXTERNAL ABORT** (SEA) when the error that it detects is an architecturally executed instruction (typically a load) that has not retired.
- An **ASYNCHRONOUS EXTERNAL ABORT** (AEA), reported as an **ERROR INTERRUPT** (SEI) when the error it detects cannot be associated with a specific instruction (typically an already retired

store). The error is Uncontainable, because it is reported asynchronously and the Cortex®-R82AE processor cannot guarantee that subsequent instructions have not consumed corrupted data.

## 10.7 Error detection and reporting

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

Any detected error is reported in the Error Record Primary Status Register (ERR<n>STATUS), and the Error Record Miscellaneous Register 0 (ERR<n>MISCO). Errors reported include errors that are successfully corrected and errors that cannot be corrected. If multiple errors occur on the same clock cycle, the Cortex®-R82AE processor serializes them and records them separately. In the unusual case when multiple errors from multiple RAMs occur in consecutive clock cycles and the Cortex®-R82AE processor cannot record them in a timely manner, the error type is set appropriately to indicate that multiple errors have been observed.

Simultaneous errors in different RAMs get serialized and reported but multiple errors within a single RAM such as multiple DTCM errors, are combined into a suitable multiple error report.

There are 10 Error Record registers, Error Record registers 0 to 9, provided, which can be selected with the ERRSELR\_EL1 register:

- Error Record register 0 is for the cluster and is shared between all cores in the cluster. It records non-ECC memory system errors in the L2 cache and LCU.
- Error Record registers 1-3 are private to each core, and are updated on any Error Correcting Code (ECC) error in the core RAMs including L1 data cache RAMs, L1 instruction cache RAMs, TCMs (ITCM and DTCM), and the L2 TLB RAMs.
- Error Record registers 4-6 are for the cluster and are shared between all cores in the cluster. They record any ECC error in the L2 cache data RAMs, L2 cache tag RAMs, L2 cache data buffer RAMs, L2 cache duplicate L1 tag RAMs, and the LCU duplicate L1 tag RAMs.
- Error Record register 7 is private to each core. It records bus protection and bus timeout errors from the Low-latency Peripheral Port (LLPP), and errors from the livelock detector and transient fault protection logic.
- Error Record registers 8-9 are for the cluster and shared between all cores in the cluster. It records bus timeout errors from the Main Manager (MM), Low-latency RAM (LLRAM) and Shared Peripheral Port (SPP), as well as bus protection errors from all non-LLPP interfaces and errors from the interrupt monitor.

Detected errors are logged in the ERR<n>STATUS and ERR<n>MISCO registers. The ERR<n>STATUS registers will capture the severity of the error observed (Corrected, Deferred, Recoverable, Unrecoverable, Uncontainable), while the format for the ERR<n>MISCO registers is dependent on the node reporting the error and provides more detail on the error in question.

### 10.7.1 Node 0: Non-ECC Memory Errors

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

ERR0MISC0 provides a detailed explanation of the type of error which has occurred. No further information is provided.

### 10.7.2 Node 1: Core Memory Errors

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

ERR1MISC0 provides more detail for the ECC error which has occurred. This includes which logical memory encountered the error; L1 I-Cache, L1 D-Cache, ITCM, DTCM or MMS. It also provides information to identify the location of the error in the RAM (index, bank, way and chunk) and the type of error (1-bit, 2-bit).

### 10.7.3 Node 4: Cluster Memory Errors

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

ERR4MISC0 provides more detail for the ECC error which has occurred. This includes which logical memory encountered the error; L2 Cache Tags, L2 Duplicate L1 Tags, L2 Cache Data, L2 Data Buffers, LCU Duplicate L1 Tags. It also provides information to identify the location of the error in the RAM (index, bank, way and chunk) and the type of error (1-bit, 2-bit).

### 10.7.4 Node 7: Core Safety Mechanism Errors

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

ERR7MISC0 provides more detail on the non-ECC safety mechanism error which has occurred including the affected interface and channel/design unit.

### 10.7.5 Node 8: Cluster Safety Mechanism Errors

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

ERR7MISC0 provides more detail on the non-ECC safety mechanism error which has occurred including the affected interface and channel/design unit.



## 10.7.6 Performance monitoring

When the Cortex®-R82AE processor consumes an error, it raises different exceptions depending on the error type.

All detected memory errors trigger the MEMORY\_ERROR event.

The MEMORY\_ERROR event is:

- Counted by the PMU counters if it is selected and the counter is enabled.
- Connected to the **EMBEDDED TRACE MACROCELL** (ETM) as external event number 28.

## 10.8 Error injection

Error injection involves inserting an error in the error reporting logic to verify the reporting and recording structure. Error injection does not verify syndrome generation or error detection and correction hardware.

Error injection uses the ERR<n>PFGCDN\_EL1 and ERR<n>PFGCTL\_EL1 registers to insert errors.

The Cortex®-R82AE processor can inject the following error types:

- For Record 0 (shared non-ECC memory errors):
  - No fault injection supported.
- For Records 1-3 (per-core memory ECC errors):
  - A Corrected error (CE); this will be reported as a single-bit ECC error upon a L1 D-Cache load access.
  - A Deferred error (DE); this will be reported as a double-bit ECC error upon a L1 D-Cache load access. If the error was detected at EL2, then the fault will also be indicated on the COREHYPERCECCFAULT pin.
  - A Recoverable error (UER) cannot be generated at this node.
  - An Unrecoverable error (UEU) cannot be generated at this node.
  - An Uncontainable error (UC); this will be reported as a double-bit ECC error upon an L1 D-Cache Main Memory eviction.
- For Records 4-6 (shared memory ECC errors):
  - A Corrected error (CE); this will be reported as a single-bit ECC error upon any L2 Cache data access.
  - A Deferred error (DE); this will be reported as a double-bit ECC error upon any L2 Cache data access.
  - A Recoverable error (UER) cannot be generated at this node.
  - An Unrecoverable error (UEU); this will be reported as a double-bit ECC error upon any L2 Cache tag access when IMP\_CLUSTERACTLR\_EL1.L2EC = 1. If IMP\_CLUSTERACTLR\_EL1.L2EC = 0 an Unrecoverable Error (UEU) cannot be generated at this node.

- An Uncontainable error (UC); this will be reported as a double-bit ECC error upon any L2 Cache tag access `IMP_CLUSTERACTLR_EL1.L2EC = 0`. If `IMP_CLUSTERACTLR_EL1.L2EC = 0` an Uncontainable Error (UC) cannot be generated at this node.
- For Record 7 (per-core safety mechanism errors):
  - A Corrected error (CE) cannot be generated at this node.
  - A Deferred error (DE) cannot be generated at this node.
  - A Recoverable error (UER); this will be reported as a detected livelock.
  - An Unrecoverable error (UEU) cannot be generated at this node.
  - An Uncontainable error (UC); this will be reported as a flop parity failure in the DPU. The fault will also be indicated on the `CORETFPFAULT` pin.
- For Record 8 and 9, present when the bus protection is included (shared bus errors):
  - A Corrected error (CE) cannot be generated at this node.
  - A Deferred error (DE) cannot be generated at this node.
  - A Recoverable error (UER) cannot be generated at this node.
  - An Unrecoverable error (UEU) cannot be generated at this node.
  - An Uncontainable error (UC); this will be reported as a bus protection error within the PPU, if `BUS_PROTECTION=1`. If `BUS_PROTECTION=0` an Uncontainable Error (EC) cannot be injected at this node.
  - The fault will also be indicated on the `CLUSTERBUSPROTFault` pin.

An error can be injected immediately, subject to the triggering condition associated with each error type, or when a 32-bit counter reaches zero. You can control the value of the counter through the `ERR<n>PFGCDN_EL1` register. The value of the counter decrements on a per clock cycle basis.

Error injection is a separate source of error within the system and does not create hardware faults.

An example software sequence to insert an error could look like this:

1. Select the appropriate RAS node by programming `ERRSELR_EL1`
2. Enable error reporting by programming `ERXCTLR_EL1`
3. Write a countdown value to `ERXPFGCDN_EL1`
4. Select an error to be injected by programming `ERXPFGCTL_EL1`
5. Ensure the programming is applied by executing a DSB and then an ISB instruction
6. After the countdown to complete, error results should be visible by reading `ERXSTATUS_EL1` and `ERXMISCO_EL1`

## 10.9 RAS register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor AArch64 *Reliability, Availability, and Serviceability* (RAS) registers in [A.1.7 AArch64 RAS registers summary](#) on page 325.

You can find the register summary table for the Cortex®-R82AE processor external RAS registers in [B.1.1.1 External RAS registers summary](#) on page 1498.

# 11. GIC CPU interface

This chapter describes the Cortex®-R82AE processor implementation of the Arm *Generic Interrupt Controller* (GIC) CPU interface.

## 11.1 About the GIC CPU interface

The GIC CPU interface, when integrated with an external GIC distributor, is a resource for supporting and managing interrupts in a cluster system.

Each core within the Cortex®-R82AE processor has a GIC CPU interface that includes registers to mask, identify, and control states of interrupts forwarded to a core. The GIC CPU interface, among other functions, turns external GIC distributor interrupt requests into IRQ and FIQ interrupts into the core.

A core accesses its GIC CPU interface registers via System register operations. Because the GIC CPU interface resides within the core, it is clock gated during WFI and WFE exceptions or placed into retention when the rest of the core enters retention. Any communication from the external GIC distributor causes a temporary wakeup or retention exit.

The Cortex®-R82AE processor has a single shared pair of bidirectional AXI5-Stream interfaces that is internally connected to all cores. The Cortex®-R82AE processor can be directly connected to an external GICv3 interrupt distributor within the system through AXI5-Stream interface.



The GIC AXI5-Stream interfaces operate in the same SCLK clock domain with the cluster. To support an integer ratio (for example, 2:1) for the GIC distributor, a clock enable signal ACLKENG is provided.

---

The external GIC distributor is responsible for receiving interrupts, prioritizing them and routing them to the associated interrupt input of the associated core within the Cortex®-R82AE processor. The software is responsible for generating interrupts for inter-core communication by writing to the interrupt controller. Local peripherals, such as the timer, have dedicated interrupts inputs that are specific to the individual core.

The Cortex®-R82AE processor conforms to the Arm GICv3.2 architecture. The Cortex®-R82AE processor implements the GIC CPU interface as described in the *Arm® Generic Interrupt Controller Architecture Specification*. This chapter describes only features that are specific to the Cortex®-R82AE processor implementation.

The Cortex®-R82AE processor implementation of GICv3.2 architecture supports:

- Single Security state.
- Interrupt virtualization.
- *Software-generated Interrupts* (SGIs).

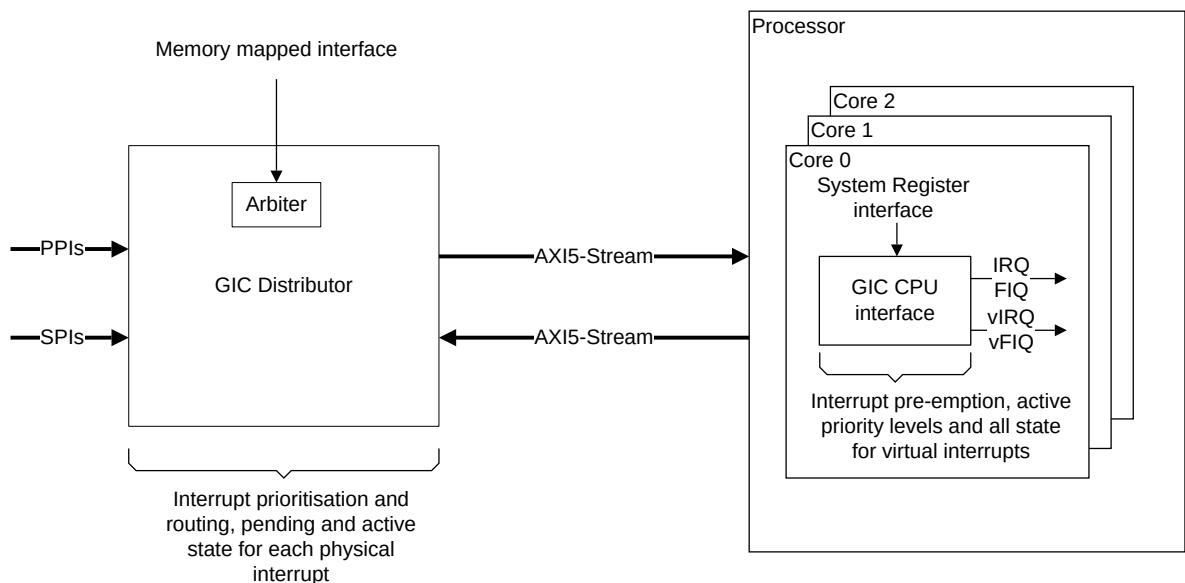
- Message Based Interrupts.
- System register access for the CPU interface.
- Interrupt masking and prioritization.
- Cluster environments, including systems that contain more than eight cores.
- Wake up events in power management environments.

The Cortex®-R82AE processor GIC CPU interface includes interrupt grouping functionality that supports:

- Configuring each interrupt to belong to an interrupt group.
- Signaling Group 1 interrupts to the target core using the IRQ exception request only.
- Signaling Group 0 interrupts to the target core using the FIQ exception request only.
- A unified scheme for handling the priority of Group 0 and Group 1 interrupts.

The following figure shows GIC CPU interface.

**Figure 11-1: GIC CPU interface**



## 11.2 Disabling the GIC CPU interface

The Cortex®-R82AE processor always includes the *Generic Interrupt Controller* (GIC) CPU interface, however you can disable it to meet your requirements.

You can disable the GIC CPU interface by asserting the GICCDISABLE signal HIGH at reset. Disabling the GIC CPU interface this way enables you to use other GIC architectures other than the GICv3.

If the Cortex®-R82AE processor is not integrated with an external GICv3 interrupt distributor component in the system, then you need to disable the GIC CPU interface. If you disable the GIC CPU interface, then:

- The input signals nIRQ, nFIQ, nVIRQ, and nVFIQ can be driven by an external GIC in the system.
- GIC System register accesses generate **UNDEFINED** instruction exceptions.

## 11.3 Bypassing the GIC CPU interface

When the GIC CPU interface is enabled (GICCDISABLE signal LOW at reset), the Cortex®-R82AE processor supports interrupt bypassing according to the GICv3 architecture.

You can use the ICC\_SRE\_EL2.DFB and ICC\_IGRPEN0\_EL1.Enable controls to bypass FIQ handling by the GIC. If you program the GIC CPU interface to bypass FIQ interrupts, the Cortex®-R82AE processor routes the nFIQ and nVFIQ input signals directly to the CPU.



When the GIC CPU interface does not bypass IRQ interrupts, the input signals nVIRQ and nIRQ are ignored.

---

You can use the ICC\_SRE\_EL2.DIB and ICC\_IGRPEN1\_EL1.Enable controls to bypass IRQ handling by the GIC. If you program the GIC CPU interface to bypass IRQ interrupts, the Cortex®-R82AE processor routes the nIRQ and nVIRQ input signals directly to the CPU.



When the GIC CPU interface does not bypass FIQ interrupts, the input signals nVFIQ and nFIQ are ignored.

---

For more information on programming the GIC CPU interface, see the [Arm® Generic Interrupt Controller Architecture Specification, GIC architecture version 3 and version 4](#).

## 11.4 GIC CPU interface register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor *Generic Interrupt Controller* (GIC) CPU interface registers in [A.1.6 AArch64 GIC system registers summary](#) on page 323.

## 12. Generic Timer

This chapter describes the Cortex®-R82AE processor implementation of the Arm Generic Timer.

### 12.1 About the Generic Timer

The Generic Timer can schedule events and trigger interrupts based on an incrementing counter value. It generates timer events as active-LOW interrupt outputs and event streams.

The Cortex®-R82AE processor Generic Timer is compliant with the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

This chapter describes only features that are specific to the Cortex®-R82AE processor implementation.

### 12.2 Generic Timer functional description

The Cortex®-R82AE processor provides a set of timer registers within each core in the cluster.

The timers are:

- An EL1 physical timer
- A Secure EL2 physical timer
- An EL1 virtual timer

The Cortex®-R82AE processor does not include the system counter. This resides in the SoC. The system counter value is distributed to the Cortex®-R82AE processor with a synchronous binary encoded 64-bit bus, CNTVALUEB[63:0].

When self-hosted trace is enabled, the system generic timer (physical or virtual) is used by the *Embedded Trace Macrocell* (ETM) for timestamp trace. When self-hosted trace is disabled, the CoreSight™ time value is identical to the system physical time value.

### 12.3 Generic Timer register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor Generic Timer registers in [A.1.10 AArch64 Generic Timer registers summary](#) on page 329.



# 13. Debug

This chapter describes the debug features of the Cortex®-R82AE processor and the associated DebugBlock component.

## 13.1 About debug methods

The Cortex®-R82AE processor supports two methods of invasive debugging to support software debugging, external debug and self-hosted debug. This section provides a brief introduction to these methods and outlines their main components.

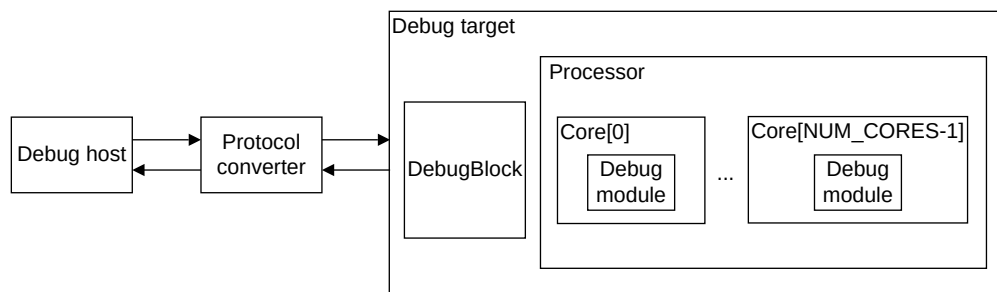
### External debug

External debug is a conventional setup for debug, in which the debugger is external to the core that is being debugged. The debugger might be either hosted on another core within the Cortex®-R82AE processor, or running external to the Cortex®-R82AE processor. For example, the debugger might be hosted on a workstation connected using JTAG to a development system containing the Cortex®-R82AE processor.

External debug is useful for hardware bring-up of a Cortex®-R82AE processor-based system, that is, debugging during development when a system is first powered up and not all of the software functionality is available.

The following figure shows a typical external debug system.

**Figure 13-1: External debug system**



### Debug host

The debug host is a computer, for example a personal computer, that is running a software debugger such as the DS-5 Debugger. With the debug host, you can issue high-level commands, such as setting a breakpoint at a certain location or examining the contents of a memory address.

## Protocol converter

The debug host sends messages to the debug target using an interface such as Ethernet. However, the debug target typically implements a different interface protocol such as JTAG or SWD. A device such as DSTREAM is required to convert between the two protocols.

## Debug target

The debug target is the lowest level of the system. An example of a debug target is a development system with a test chip or a silicon part with a Cortex®-R82AE processor. The debug target implements system support for the protocol converter to access the Cortex®-R82AE Debug modules.

## Debug module

The debug modules within the Cortex®-R82AE processor help with debugging software that is running on the processor such as an operating system or application software.

The debug modules enable an external debugger to:

- Stop program execution.
- Examine and alter processor state.
- Examine and alter memory and the state of the input or output peripherals.
- Restart the core.

## Self-hosted debug

In self-hosted debug, the core being debugged within the Cortex®-R82AE processor hosts debug monitor software itself. Hardware watchpoints and breakpoints generate debug exceptions on debug events.

Self-hosted debug is useful in situations in which the Cortex®-R82AE processor has been deployed in a developed system, where there is no direct access to the Cortex®-R82AE processor debug hardware. Self-hosted debug supports:

- Task debugging.
- OS and kernel debugging.
- Hypervisor debugging. Self-hosted debug support for Hypervisor code is limited to software breakpoint instructions.

For more information, see [13.4 Debug events](#) on page 267. These exceptions are handled by the debug monitor that typically resides alongside the operating system kernel or the hypervisor.

For details on self-hosted debug, see [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

## 13.2 Debug functional description

This section describes the trace, debug, and test features supported by the Cortex®-R82AE processor. It includes Arm®v8-R AArch64 debug, cache debug, and CoreSight™ debug.

### Arm®v8-R AArch64 debug architecture support

The Cortex®-R82AE processor implements the Arm®v8-R AArch64 debug architecture including debug features up to Arm®v8.4 and the debug over powerdown Armv8.3-DoPD feature.

The Cortex®-R82AE processor allows access to the internal debug functionality and registers either through a memory-mapped area on the external AMBA® APB5 completer port or by using System register operations from software running on the Cortex®-R82AE processor.

Each core within the Cortex®-R82AE processor implements six hardware breakpoints, four watchpoints, and a *Debug Communications Channel* (DCC). Four of the breakpoints match only against virtual address, the other two breakpoints match against either virtual address or context ID. All watchpoints can be linked to either of the virtual address or context-ID matching breakpoints to allow a memory request to be trapped in a given process context.

### Cache debug

Cache debug allows software to read the content of the L1 cache, L2 cache, L2 duplicate L1 tag RAMs, and *LLRAM Coherency Unit* (LCU) duplicate L1 tag RAMs through **IMPLEMENTATION DEFINED** System registers.

See [8.12 Direct access to internal memories](#) on page 197 for more information on the mechanisms the Cortex®-R82AE processor provides to read the internal memories.

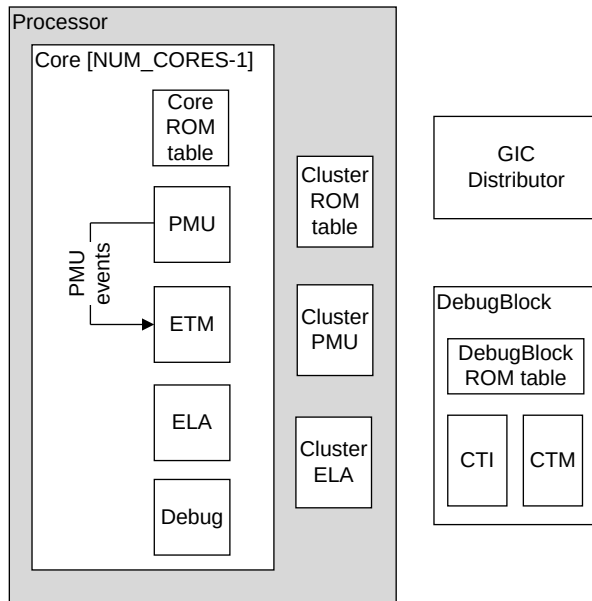
### CoreSight™ debug

The Cortex®-R82AE processor integrates several CoreSight™ debug related components to aid system debug along with CoreSight™ SoC.

These components include:

- Per-core *Embedded Trace Macrocell* (ETM).
- Per-core and a cluster level *Cross Trigger Interface* (CTI).
- *Cross Trigger Matrix* (CTM).
- Per-core and a cluster level *Performance Monitoring Unit* (PMU).
- Support for per-core and a cluster level CoreSight™ ELA-600 *Embedded Logic Analyzer*.
- Debug over powerdown support.
- Per-core ROM table, cluster ROM table, and DebugBlock ROM table.

The following figure shows the Cortex®-R82AE processor CoreSight™ debug components.

**Figure 13-2: Debug system components**

The debug components are split into two groups. Some components are in the cluster itself and the rest are in a separate block named the DebugBlock. Separating the DebugBlock from the Cortex®-R82AE processor allows you to put the DebugBlock in a separate power domain and place it physically with other CoreSight™ logic in the SoC, rather than close to the cluster. It also allows you to implement the debug components in an always on power domain, enabling debug over powerdown.

The connection between the cluster and the DebugBlock consists of a pair of APB interfaces, one in each direction. All debug traffic, except the authentication interface, takes place over this interface as read or write APB transactions. It includes register reads, writes, and CTI triggers. For more information, see [13.5 The DebugBlock](#) on page 268.

All debug components are controlled through the primary Debug APB interface on the DebugBlock. Requests on this bus are decoded by the APB decoder before being sent to the appropriate component in the DebugBlock or in the cluster. The per-core CTIs and the cluster CTI are connected to a CoreSight™ CTM.

Each core within the Cortex®-R82AE processor contains an ETM, PMU, optional ELA, and debug component that are accessed using the debug APB bus. This block conforms to the Arm®v8-R AArch64 Debug Architecture Specification.

When the Cortex®-R82AE processor is configured to include the optional ELA-600 instances, a number of key internal processor signals become observable. In the unlikely case where a processor bug is suspected, the Arm support team may provide programming sequences for ELA-600 and then analyze the captured data streams. Adding the optional ELA capabilities to the existing

Debug, PMU and Trace logic and combining triggers through the Cross-Trigger Matrix increase the likelihood of successfully debugging difficult and rare hardware issues.



The CoreSight ELA-600 is a separately licensable product.

The ETM in each core produces two separate instruction and data trace streams. The optional ELA in each core and the optional cluster ELA also produce data streams. All the core and cluster streams are combined and are output from the Cortex®-R82AE processor using one AMBA® 4 ATB 32-bit interface (for ETM instruction trace streams) and one AMBA® 4 ATB 128-bit interface (for ETM data trace streams and ELA streams).

When an ELA is active, the relevant core or cluster clock will remain on and the associated logic will be unable to enter a low power state.

## 13.3 Debug register accesses

The Cortex®-R82AE processor implements the Arm®v8-R AArch64 Debug architecture and debug events.

They are described in the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

The Debug architecture defines a set of debug registers. The debug registers can be accessed from:

- Software running on the core.
- An external debugger.

### 13.3.1 Processor accesses

System register access allows the Cortex®-R82AE processor to directly access certain Debug registers through the use of dedicated system instructions (`MSR` and `MRS` instructions).

The external debug interface enables debug agents running on a core within the Cortex®-R82AE processor to access the Debug registers. Access to the debug registers is partitioned as follows:

#### Debug registers

This function is System register based. You can access the core Debug registers by using the dedicated system registers. See [13.7 Debug register summary](#) on page 274 for more information on Debug registers.

### Performance Monitors registers

This function is System register based. You can access both the core and cluster Performance Monitors registers by using the dedicated system registers. See [14.6 PMU register summary](#) on page 293 for more information on Performance Monitors registers.

### Trace registers

This function is System register based. You can access the core trace registers by using the dedicated system registers. See [15.6 ETM register summary](#) on page 304 for more information on trace registers.

## 13.3.2 Effects of resets on Debug registers

Core and cluster Cold resets and Warm resets that are generated by programming the *Power Policy Units* (PPUs) affect the Debug related registers.

A core Cold reset affects all resettable registers in a specific core including the debug, *Embedded Trace Macrocell* (ETM), and *Reliability, Availability, and Serviceability* (RAS) registers.

A core Warm reset affects all resettable registers in a specific core except the debug, ETM, and RAS registers.

A cluster Cold reset affects all resettable registers in the Cortex®-R82AE processor and the DebugBlock except the *Power Policy Unit* (PPU).

A cluster Warm reset affects all resettable registers in the Cortex®-R82AE processor except the DebugBlock, PPU, Utility bus, debug, ETM, and RAS registers.

See [6.7 Explicit resetting of cluster and cores and debug recovery](#) on page 105 for more information for reset control with the PPU.

## 13.3.3 External access permissions to debug registers

External access permission to the Debug registers depends on the conditions at the time of the access.

The following table describes the Cortex®-R82AE processor response to accesses through the external debug interface for different access conditions.

**Table 13-1: External access conditions to registers**

Name	Condition	Effect on access permissions
Off	Core power domain is On as indicated by reading EDPRSR.PU as 1	Access to this field of the EDPRSR register is <i>Read-As-One</i> (RAO) in accordance with Armv8.3 debug over powerdown.  When the core power domain is in a powerup state, the debug registers in the core power domain can be accessed.  When the core power domain is Off, accesses to the debug registers in the core power domain, including EDPRSR, return an error.
OSLK	OSLSR_EL1.OSLK is 1	OS Lock is locked.
EDAD	<code>AllowExternalDebugAccess() == FALSE</code>	External debug access is disabled for Non-secure accesses to this register. This causes an error for certain reads and writes to Debug registers through the external debug interface.  When an error is returned because of an EDAD condition code, and this is the highest priority error condition, EDPRSR.SDAD is set to 1. Otherwise SDAD is unchanged.
Default	-	None of the conditions apply. This is normal access.

### 13.3.4 Breakpoints and watchpoints

The Cortex®-R82AE processor supports six breakpoints, four watchpoints, and a standard *Debug Communications Channel* (DCC).

A breakpoint control register (DBGBCR<n>\_EL1) and a breakpoint value register (DBGBVR<n>\_EL1) forms a breakpoint<n> where <n> is 0-5. These two registers are referred to as a *Breakpoint Register Pair* (BRP).

Four of the breakpoints (BRP 0-3) match only to the virtual address and the other two (BRP 4 and 5) match against either the *Virtual Address* (VA) or context ID, or the *Virtual Machine ID* (VMID). All the watchpoints can be linked to two breakpoints (BRP 4 and 5) to enable a memory request to be trapped in a given process context.

## 13.4 Debug events

A debug event can be either a software debug event or a halting debug event.

The Cortex®-R82AE processor responds to a debug event in one of the following ways:

- It ignores the debug event.
- It takes a debug exception.
- It enters debug state.

See the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#) for more information about the debug events.

### 13.4.1 Watchpoint debug events

Watchpoint debug events are always synchronous in the Cortex®-R82AE processor.

Memory hint instructions and cache clean operations, except `DC ZVA` and `DC INVAC`, do not generate watchpoint debug events. Store exclusive instructions generate a watchpoint debug event even when the check for the control of exclusive monitor fails. Atomic CAS instructions generate a watchpoint debug event even when the compare operation fails.

### 13.4.2 Debug OS Lock

Debug OS Lock is set by the core Cold reset and cluster Cold reset.

For normal behavior of debug events and Debug register accesses, Debug OS Lock must be cleared either through self-hosted debug performing a System register access or through external debug.

For more information, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

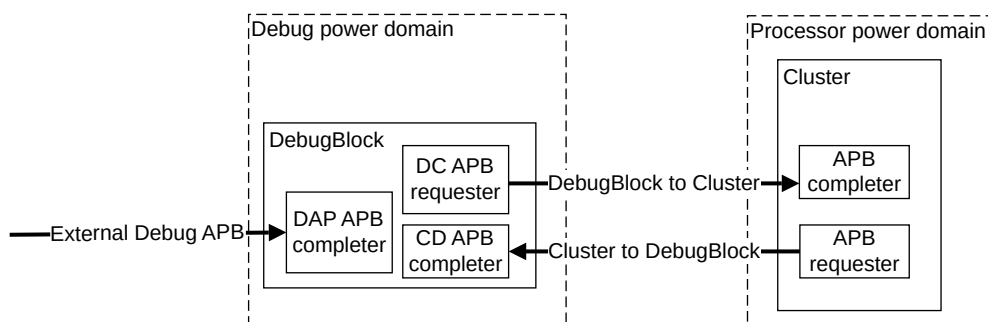
## 13.5 The DebugBlock

The DebugBlock combines the functions, registers, and interfaces that are required for debug over powerdown.

The DebugBlock is provided as a separate component to allow implementation of it in a separate power domain from the cluster. Having a separate debug power domain allows the connection to a debugger be maintained while the Cortex®-R82AE processor is powered down. The Cortex®-R82AE processor also allows powering down the DebugBlock when debug is not in process.

The following diagram shows how the DebugBlock is connected to the cluster.

**Figure 13-3: Debug APB connections**



The DebugBlock has three APB interfaces:



### External Debug APB (DAP APB)

An AMBA® APB5 completer interface, allowing communication with an external debugger, for example through a CoreSight™ *Debug Access Port* (DAP).

All debug register read and write requests from an external debugger are received on this bus.

Bus Protection is not provided on this interface since the debug block is expected to be powered down when fault detection is required.

### DebugBlock to cluster (DC APB)

An AMBA® APB5 requester interface that is connected to the cluster. It sends all debug register read and write requests to the cluster.

CTI output trigger events are sent to the cluster as trigger event requests on this bus.

When the processor is configured for bus protection, the PSELDC and PENABLEDC inputs to the processor are protected with odd parity.

### Cluster to DebugBlock (CD APB)

An AMBA® APB5 completer interface that is connected to the cluster. It receives CTI input trigger event requests from the cluster.

When the processor is configured with bus protection, the PREADYCD and PSLVERRCD inputs to the processor are protected with odd parity.

### Debug register reads and writes

The DebugBlock holds all the debug registers that are implemented in the Debug power domain. Registers implemented in the Debug power domain are specified in the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

Accesses through the DAP APB interface to Debug power domain registers are handled internally by the DebugBlock. Accesses through the DAP APB interface to processor power domain (PDCLUSTER or PDCPU<m>) registers are passed on to the cluster through the DC APB interface.

### CTI trigger events

Trigger events are transferred between the DebugBlock and cluster through the CD APB and DC APB interfaces.

### Input trigger events

Input trigger events are sent from the cluster to the CTIs through the CD APB as write transactions.

### Output trigger events

Output trigger events are sent from the CTIs to the cluster through the DC APB multicast trigger requests..

### DebugBlock power states

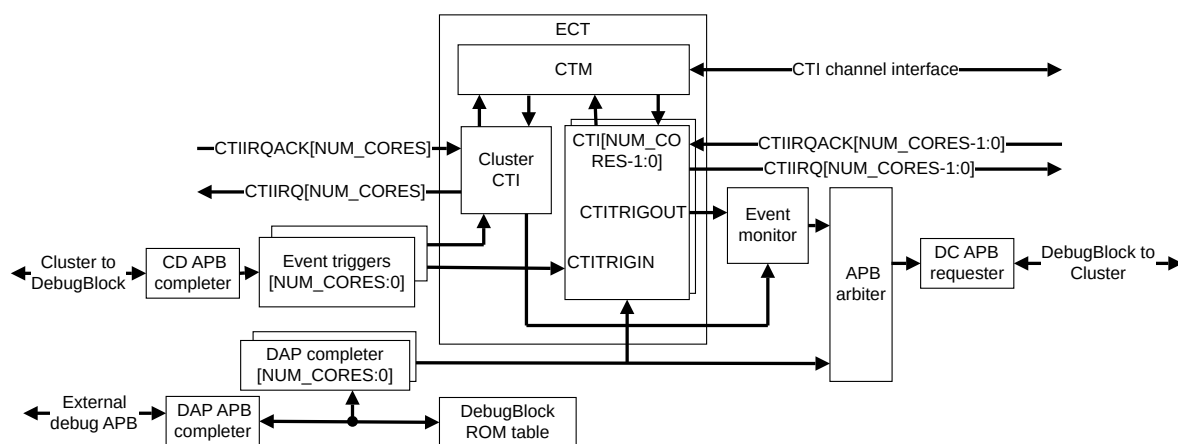
The DebugBlock supports two power modes: ON, and OFF. The DebugBlock sends powerup and powerdown requests to the external power controller on its external Q-Channel interface. In the OFF mode, the DebugBlock does not initiate any APB accesses and all incoming APB accesses to the DebugBlock receive a PSLVERR response.

When the processor is in Lock or Hybrid mode, a debug inadvertent activation fault will be flagged by the DCLS logic if the debug block is powered on or if a trigger event is sent on the CD APB interface.

### 13.5.1 DebugBlock components

The following figure shows the DebugBlock components.

**Figure 13-4: DebugBlock block diagram**



The CTIs shown in the diagram includes both the CTIs attached to each of the cores [NUM\_CORES-1:0] and the cluster CTI. NUM\_CORES has a value of the total number of cores that are implemented.

## ECT

The DebugBlock implements the *Embedded Cross Trigger* (ECT).

## DebugBlock ROM table

The DebugBlock ROM table holds the address decoding for each debug component in the DebugBlock and one entry pointing to the cluster ROM table. The DebugBlock ROM table complies with the [Arm® CoreSight™ Architecture Specification v3.0](#) and supports the v8 debug address map.

## Event monitor

The event monitor converts changes in CTI output triggers to APB write transactions.

## Event triggers

The event triggers convert APB write transactions to CTI input triggers.

## APB arbiter

The DC APB transfers both register accesses and CTI output trigger events. The APB arbiter multiplexes the two sources of transactions.

## DAP completer

The DAP completer holds copies of registers in the debug power domain.

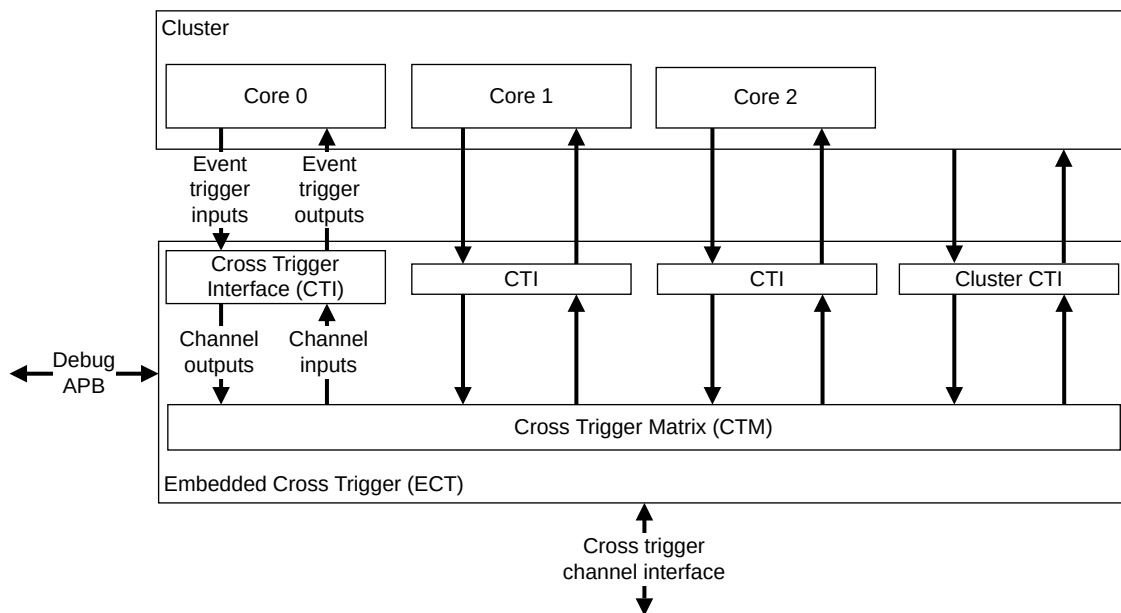
## 13.6 ECT

The *Embedded Cross Trigger* (ECT) allows debug events to be sent between the cores within the Cortex®-R82AE processor.

The ECT provides a *Cross Trigger Interface* (CTI) for each core in the cluster and a CTI at the cluster level. The CTIs are interconnected through a *Cross Trigger Matrix* (CTM) implemented at the DebugBlock to send debug and trace events between the cores.

The following diagram shows a conceptual view of the trigger event inputs and outputs between the cores and ECT.

**Figure 13-5: Embedded Cross Trigger concept**



The CTIs selectively send trigger events to the CTM on their respective channel outputs. The CTIs receive trigger events from the CTM on their channel inputs.

Trigger events are transferred between CTIs over the channel interface. The CTM connects the channel interface to the channel inputs and channel outputs of the CTIs.

## External interfaces

The external cross-trigger channel interface, from the CTM, allows cross-triggering between SoC external devices.

The Debug APB provides access to the CTI registers. This allows an external debugger to configure the trigger event routing, and send events to cores, for example, to put a core into Debug state.

## CTI registers

Registers in the CTI:

- Control the mapping of the input trigger events to channel outputs.
- Control the mapping of the channel inputs to output trigger events.
- Capture the state of input and output trigger events.
- Set, clear, or pulse output trigger events.

### 13.6.1 Supported debug and trace trigger events

The CTIs each have ten input and output trigger events that are mapped onto the debug and trace events in the cores and ELAs.

#### From the CTI to the core

The debug and trace trigger events from the CTI to the core are:

##### Debug request trigger event

A trigger event sent from the CTI to the core to force the core into Debug state.

##### Restart request trigger event

A trigger event sent from the CTI to the core to request the core to exit Debug state.

##### Generic CTI interrupt trigger event

A trigger event sent from the CTI to the GIC.

##### ETM trace input trigger events

Four trigger events sent from the CTI to the ETM trace in the core.

##### ELA input trigger events

Two trigger events sent from the CTI to the ELA attached to the core. If there is no ELA, the ELA trigger events are tied LOW.

#### From the core to the CTI

The debug and trace events from the core to the CTI are:

##### Cross-halt trigger event

A trigger event sent from the core to the CTI when the core enters Debug state.

##### Performance Monitoring Unit (PMU) overflow trigger event

A trigger event sent from the core to the CTI when a PMU counter overflows.

**ETM trace output trigger events**

Four trigger events sent from the ETM in the core to the CTI.

**ELA output trigger events**

Two trigger events sent from the ELA (attached to the core) to the CTI.

Similar to core CTIs, the cluster CTI has ten input and output trigger events. However, only the PMU, Generic CTI, and ELA entries are relevant. This is because there is a PMU and an ELA component at the cluster level, but there are no cluster debug and ETM components.

**From the cluster CTI to the cluster**

The trigger events from the cluster CTI to the cluster are:

**Generic CTI interrupt trigger event**

A trigger event sent from the cluster CTI to the cluster GIC.

**Cluster ELA input trigger events**

Two trigger events sent from the cluster CTI to the cluster ELA.

**From the cluster to the cluster CTI**

The trigger events from the cluster to the cluster CTI are:

**PMU overflow trigger event**

A trigger event sent from the cluster to the cluster CTI when the cluster PMU counter overflows.

**Cluster ELA output trigger events**

Two trigger events from the cluster ELA to the cluster CTI.

## 13.6.2 CTI triggers

The DebugBlock implements a *Cross Trigger Interface* (CTI) per core and a CTI for the cluster. Each CTI has 10 CTI inputs and 10 CTI output triggers. All cores in the Cortex®-R82AE processor have the same CTI trigger mapping.

**Core CTI input trigger events**

The following table shows how events are mapped onto core CTI input triggers.

**Table 13-2: Allocation of core CTI trigger inputs**

Trigger number	Source	Destination	Type	Event description
0	Core Debug	CTI	Pulse	Cross-halt trigger event
1	Core PMU	CTI	Pulse	Performance Monitoring Unit (PMU) Overflow trigger event
2-3	-	-	-	Reserved
4-7	Core ETM	CTI	Pulse	<i>Embedded Trace Macrocell</i> (ETM) trace external output trigger events
8-9	Core ELA	CTI	Pulse	<i>Embedded Logic Analyzer</i> (ELA) CTTRIGOUT[1:0] trigger events

## Core CTI output trigger events

The following table shows how events are mapped onto core CTI output triggers.

**Table 13-3: Allocation of core CTI trigger outputs**

Trigger number	Source	Destination	Type	Event description
0	CTI	Core Debug	Level	Debug Request trigger event
1	CTI	Core Debug	Pulse	Restart Request trigger event
2	CTI	GIC	Pulse	Generic CTI Interrupt trigger event
3	-	-	-	Reserved
4-7	CTI	ETM	Pulse	ETM trace external input trigger events
8-9	CTI	ELA	Pulse	ELA CTTRIGIN[1:0] trigger events

## Cluster CTI input trigger events

The following table shows how events are mapped onto the cluster CTI input triggers.

**Table 13-4: Allocation of cluster CTI trigger inputs**

Trigger number	Source	Destination	Type	Event description
0	-	-	-	Reserved
1	Cluster PMU	CTI	Pulse	PMU Overflow trigger event
2-7	-	-	-	Reserved
8-9	Cluster ELA	CTI	Pulse	Cluster ELA CTTRIGOUT[1:0]

## Cluster CTI output trigger events

The following table shows how events are mapped onto the cluster CTI output triggers.

**Table 13-5: Allocation of cluster CTI trigger outputs**

Trigger number	Source	Destination	Type	Event description
0-1	-	-	-	Reserved
2	CTI	GIC	Pulse	Generic CTI Interrupt trigger event
3-7	-	-	-	Reserved
8-9	CTI	Cluster ELA	Pulse	Cluster ELA CTTRIGIN[1:0]

## 13.6.3 CTI register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor *Cross Trigger Interface* (CTI) registers [B.2.1.6 External CTI registers summary](#) on page 1716.

## 13.7 Debug register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor AArch64 Debug registers in [A.1.5 AArch64 Debug registers summary](#) on page 322.

You can find the register summary table for the Cortex®-R82AE processor external Debug registers in [B.2.1.1 External Debug registers summary](#) on page 1708.

# 14. PMU

This chapter describes the *Performance Monitoring Unit* (PMU).

## 14.1 About the PMU

The Cortex®-R82AE processor includes *Performance Monitoring Units* (PMUs) to assist software profiling and performance debugging. The PMUs implement the PMUv3 architecture and include Arm®v8.4 PMU extensions.

The PMUs enable you to gather various statistics on the operation of each core and the cluster and their memory system during runtime.

The Cortex®-R82AE processor implements:

- One PMU per core to monitor events local to the core such as L1 cache linefills.
- One PMU at the cluster level to monitor events that are shared by the cores such as L2 cache linefills or *LLRAM Coherency Unit* (LCU) accesses.

Some of the events from the per-core PMUs are also exported for use by the respective Trace units.

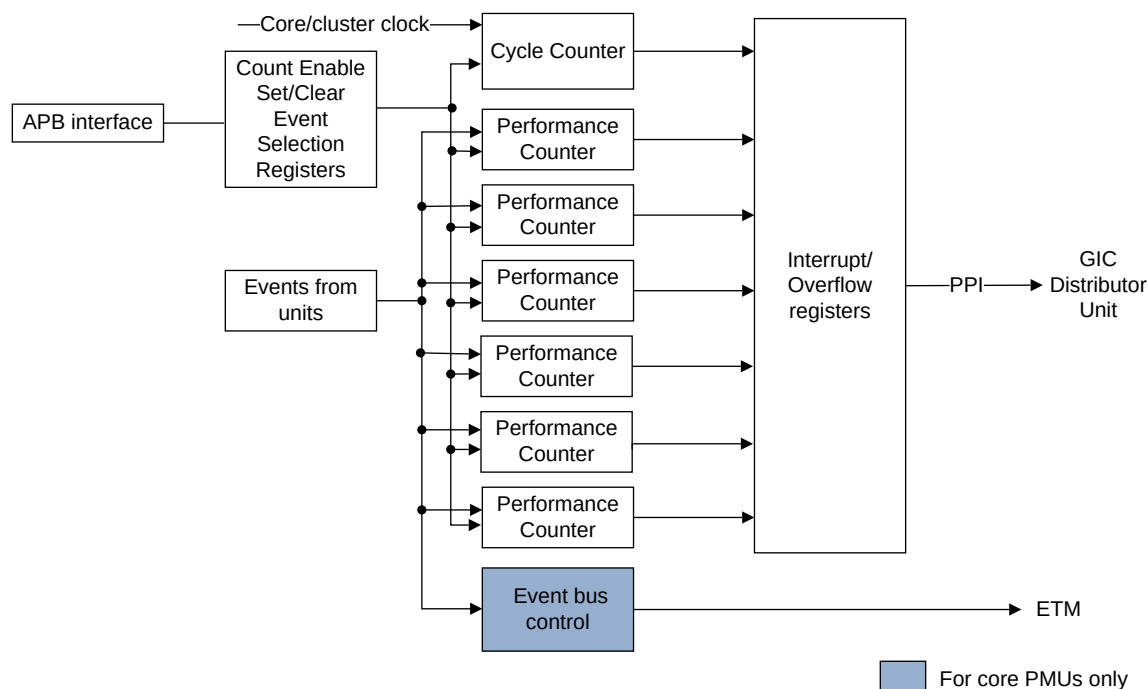
Each PMU implements six 64-bit event counters. Each counter in core PMUs can count any of the events available in that core. Each counter in the cluster PMU can count any of the events available in the cluster. The absolute counts that are recorded might vary because of pipeline effects. This has negligible effect except in cases where the counters are enabled for a very short time.

Software running on the cores in the Cortex®-R82AE processor can access the PMUs through System registers. Each core is able to access its own private PMU and the shared cluster PMU. All the core PMUs and the cluster PMU are accessible to an external agent, such as an external debug host, through the Debug APB bus.

The cluster PMU is not accessible when the cluster is in Warm reset, such as during the OFF\_EMU power mode.

The following figure shows the major blocks inside the PMU.



**Figure 14-1: PMU block diagram**

## 14.2 PMU functional description

This section describes the functionality of the PMU.

### Event interface

Events from units from across the design are provided to the PMU.

### System registers and APB interface

You can program the core and cluster PMU registers using the System registers or the external APB interface.

### Counters

The PMU has 32-bit event counters that increment when they are enabled, based on events, and a 64-bit cycle counter.

## 14.3 External register access permissions to the PMU registers

External access permission to the PMU registers is subject to the conditions at the time of the access.

The following table describes the core response to accesses through the external debug and memory-mapped interfaces.

**Table 14-1: External register conditions**

Name	Condition	Description
Off	EDPRSR.PU is 0	Access to this field is Read-As-One (RAO) in accordance with Armv8.3 debug over powerdown.  When the core power domain is in a powerup state, the PMU registers in the core power domain can be accessed.  When the core power domain is off, accesses to the PMU registers in the core power domain, including debug registers and EDPRSR, return an error.
OSLK	OSLSR_EL1.OSLK is 1	OS Lock is locked.
Default	-	None of the conditions apply, normal access.

## 14.4 PMU events

This section describes the core and cluster *Performance Monitoring Unit* (PMU) events of the Cortex®-R82AE processor.

### 14.4.1 Core PMU events

*Performance Monitoring Units* (PMUs) private to each core collect events from the units within the core and use event codes to reference these events.

Core PMU events are architecturally, microarchitecturally, or implementation defined. Architectural, microarchitectural, and implementation defined core PMU events are the same for each core within the Cortex®-R82AE processor.

### 14.4.1.1 Architectural core PMU events

The following table lists the architectural events in each core.



Some events are exported to the *Embedded Trace Macrocell* (ETM). The ETM can directly select the events based on their *Performance Monitoring Unit* (PMU) event code. You can use these events to build complex triggers.

**Table 14-2: Architectural core PMU events**

Event code	ETM code	Mnemonic	Description
0x0000	0x-	SW_INCR	Instruction architecturally executed, condition code check pass, software increment.
0x0006	0x09	LD_RETIRED	Instruction architecturally executed, condition code check pass, load. This counts all load and prefetch instructions. This includes the v8.1 atomic instructions, other than the ST* variants.
0x0007	0x0A	ST_RETIRED	Instruction architecturally executed, condition code check pass, store. This counts all store instructions, and DC ZVA. This includes all the v8.1 atomic instructions. Store-exclusive instructions which fail are not counted.
0x0008	0x0B	INST_RETIRED	Instruction architecturally executed. This counts all retired instructions, including those that fail their condition code check.
0x0009	0x0C	EXC_TAKEN	Exception taken
0x000A	0x0D	EXC_RETURN	Instruction architecturally executed, condition code check pass, exception return
0x000B	0x0E	CID_WRITE_RETIRED	Instruction architecturally executed, condition code check pass, write to CONTEXTIDR_EL1. Writes to CONTEXTIDR_EL12 are not counted.
0x000C	0x0F	PC_WRITE_RETIRED	Instruction architecturally executed, condition code check pass, software change of the PC.
0x000D	0x10	BR_IMMED_RETIRED	Instruction architecturally executed, immediate branch. ISBs are not counted.
0x000E	0x11	BR_RETURN_RETIRED	Instruction architecturally executed, condition code check pass, procedure return
0x000F	0x12	UNALIGNED_LDST_RETIRED	Instruction architecturally executed, condition code check pass, unaligned load or store
0x001C	0x1E	TTBR_WRITE_RETIRED	Instruction architecturally executed, condition code check pass, write to TTBRx_EL1.
0x001E	0x-	CHAIN	Odd performance counter chain mode
0x0021	0x21	BR_RETIRED	Instruction architecturally executed, branch. This includes any instruction that is in the branch pipeline.

### 14.4.1.2 Microarchitectural core PMU events

The following table lists the microarchitectural events in each core.

**Table 14-3: Microarchitectural core PMU events**

Event code	ETM code	Mnemonic	Description
0x0001	0x04	L1I_CACHE_REFILL	L1 instruction cache refill. Counts any instruction fetch which misses in the cache and starts a new cache refill. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted. This event counts the sum of MM_L1I_CACHE_REFILL and LLRAM_L1I_CACHE_REFILL.
0x0002	0x05	L1I_TLB_REFILL	L1 instruction TLB refill. Counts any refill of the instruction L1-MMS from the L2 MMS. This includes refills which result in a translation fault. This includes accesses to either the MPUs or the TLB. TLB maintenance instructions are not counted. This event counts regardless of whether translation is enabled.
0x0003	0x06	L1D_CACHE_REFILL	L1 data cache refill. Counts any load or store operation or pagewalk access which causes data to be read from outside the L1, including accesses which do not allocate into L1. Cache maintenance instructions and prefetches are not counted. Stores of an entire cache line are not counted, even if they make a coherency request outside the L1. Partial cache line writes which do not allocate into the L1 cache are not counted. Non-cacheable accesses are not counted. This event counts the sum of L1D_CACHE_REFILL_RD and L1D_CACHE_REFILL_WR.
0x0004	0x07	L1D_CACHE	L1 data cache access. Counts any load or store operation or pagewalk access which looks up in the L1 data cache. In particular, any access which could increment the L1D_CACHE_REFILL event causes this event to count. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted. This event counts the sum of L1D_CACHE_RD and L1D_CACHE_WR.
0x0005	0x08	L1D_TLB_REFILL	L1 data TLB refill. Counts any refill of the data L1-MMS from the L2 MMS. This includes refills which result in a translation fault. TLB maintenance instructions are not counted. This event counts regardless of whether translation is enabled.
0x0010	0x13	BR_MIS_PRED	Mispredicted or not predicted branch speculatively executed. This counts any predictable branch instruction (in other words, any type of instruction that the IFU can predict) which is mispredicted (either due to dynamic misprediction, or because the MMU is off and the branches are statically predicted not taken).
0x0011	0x-	CPU_CYCLES	The number of core clock cycles. Counts even when the core is in WFI or WFE state.
0x0012	0x14	BR_PRED	Predictable branch speculatively executed. Counts all predictable branches (superset of BR_MIS_PRED).
0x0013	0x15	MEM_ACCESS	Data memory access. Counts memory accesses due to load or store instructions. Does not count instruction fetches, cache maintenance instructions, translation table walks or prefetches. This event counts the sum of MEM_ACCESS_RD and MEM_ACCESS_WR.
0x0014	0x0x16	L1I_CACHE	L1 instruction cache access. Counts any instruction fetch which accesses the L1 I-cache. Cache maintenance instructions are not counted. Non-cacheable accesses are not counted. This event is a sum of MM_L1I_CACHE and LLRAM_L1I_CACHE.
0x0015	0x17	L1D_CACHE_WB	L1 data cache write-back. Counts any write back of data from the L1 data cache to L2. This counts both victim line evictions and snoops, including cache maintenance operations. Invalidations which do not result in data being transferred out of the L1 are not counted. Does not count any full-line writes which write to L2 without writing L1 (for example, write-streaming mode).
0x0019	0x1B	BUS_ACCESS	Bus access. Counts for every beat of data transferred over the data channels between the core and the SCU. If both read and write data beats are transferred on a given cycle, this event is counted twice on that cycle. This event counts the sum of BUS_ACCESS_RD and BUS_ACCESS_WR.

Event code	ETM code	Mnemonic	Description
0x001A	0x1C	MEMORY_ERROR	Local memory error. Counts any Correctable or Uncorrectable memory error (ECC or parity) in the protected CPU RAMs. Counts only when error recording is enabled.
0x001B	0x1D	INST_SPEC	Operation speculatively executed. This event counts every instruction issued from the Iss pipeline stage.
0x001D	0x--	BUS_CYCLES	Bus cycles. The event duplicates CPU_CYCLES.
0x001F	0x1F	L1D_CACHE_ALLOCATE	L1 data cache allocation without refill. The counter increments on every attributable write that writes an entire line into the L1 cache without fetching from outside the L1 cache, for example: Writes merged to a full cache line in the store buffer or a DC ZVA operation.
0x0020	0x20	L2D_CACHE_ALLOCATE	L2 unified cache allocation without refill. The counter increments on every attributable write that writes an entire line into the L2 cache without fetching from outside the L1 or L2 cache, for example: Writes merged to a full cache line in the store buffer or a write-back from L1 to L2 cache or a DC ZVA operation.
0x0022	0x22	BR_MIS_PRED_RETIRED	Instruction architecturally executed, mispredicted branch. Counts any branch counted by BR_RETIRED which is not correctly predicted and causes a pipeline flush.
0x0023	0x23	STALL_FRONTEND	No operation issued due to the frontend. Counts on any cycle when no operations are issued due to the instruction queue being empty. This event is a sum of STALL_FRONTEND_CACHE and STALL_FRONTEND_TLB.
0x0024	0x24	STALL_BACKEND	No operation issued due to backend. Counts on any cycle when no operations are issued due to a pipeline stall. This event is a sum of all STALL_BACKEND_* events.
0x0025	0x25	L1D_TLB	L1 data TLB access. Counts any load or store operation which accesses the data L1-MMS. If both a load and a store are executed on a cycle, this event counts twice. This event counts regardless of whether translation is enabled.
0x0026	0x26	L1I_TLB	L1 instruction TLB access. Counts any instruction fetch which accesses the instruction L1-MMS. This event counts regardless of whether translation is enabled.
0x002D	0x2A	L2D_TLB_REFILL	Attributable L2 unified TLB refill. Counts on any refill of the L2 TLB, caused by either an instruction or data access. This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x002F	0x2B	L2D_TLB	Attributable L2 unified TLB access. Counts on any access to the L2 TLB (caused by a refill of any of the L1 TLBs). This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x0036	0x2C	LL_CACHE_RD	Last Level cache access, read, main manager address. If IMP_CPUECTLR_EL1.EXTLLC is set: Counts SYS_CACHE_RD. If L2 cache is present counts L2_CACHE_RD otherwise counts L1_CACHE_RD.
0x0037	0x2D	LL_CACHE_MISS_RD	Last Level cache miss, read, main manager address. If IMP_CPUECTLR_EL1.EXTLLC is set: counts SYS_CACHE_MISS_RD. If L2 cache is present counts SYS_CACHE_RD otherwise counts L1D_CACHE_REFILL_RD.
0x0038	0x19	REMOTE_ACCESS_RD	Access to another socket in a multi-socket system, read. Counts any read transaction which returns a data source of remote.
0x0039	0x--	L1D_CACHE_LMISS_RD	The counter counts each access counted by L1D_CACHE that incurs additional latency because it returns data from outside the L1 data cache. This counter does not count: A miss that does not cause a new cache refill but is satisfied from a previous miss.
0x003A	0x--	OP_RETIRED	The counter counts each operation counted by OP_SPEC that would be executed in a simple sequential execution of the program.
0x003B	0x--	OP_SPEC	The counter counts the number of operations executed by the PE, including those that are executed speculatively and would not be executed in a simple sequential execution of the program.

Event code	ETM code	Mnemonic	Description
0x003C	0x-	STALL	The counter counts every Attributable cycle on which no Attributable instruction or operation was sent for execution on this PE. This event is the union of STALL_FRONTEND and STALL_BACKEND.
0x003D	0x-	STALL_SLOT_BACKEND	Counts each slot counted by STALL_SLOT where no attributable instruction or operation was sent for execution because the backend is unable to accept one of: the instruction operation available for the PE on the slot or any operations on the slot.
0x003E	0x-	STALL_SLOT_FRONTEND	Counts each slot counted by STALL_SLOT where no attributable instruction or operation was sent for execution because there was no attributable instruction or operation available to issue from the PE from the frontend for the slot.
0x003F	0x-	STALL_SLOT	The counter counts on each attributable cycle the number of instruction or operation slots that were not occupied by an instruction or operation attributable to the PE.
0x4006	0x-	L1I_CACHE_LMISS	The counter counts each access counted by L1I_CACHE that incurs additional latency because it returns instructions from outside the L1 instruction cache. This counter does not count: A miss that does not cause a new cache refill but is satisfied from a previous miss.
0x4020	0x-	LDST_ALIGN_LAT	The counter counts each access counted by MEM_ACCESS that, due to the alignment of the address and size of data being accessed, incurred additional latency.
0x4021	0x-	LD_ALIGN_LAT	The counter counts each memory-read access counted by LDST_ALIGN_LAT.
0x4022	0x-	ST_ALIGN_LAT	The counter counts each memory-write access counted by LDST_ALIGN_LAT.

### 14.4.1.3 Implementation defined core PMU events

The following table lists the implementation defined core events and the numbers that the *Performance Monitoring Unit* (PMU) in that core uses to reference the events.

**Table 14-4: Implementation defined core PMU events**

Event code	ETM code	Mnemonic	Description
0x00C1	0x-	L2D_CACHE_REFILL_PREFETCH	A stash request to prefetch a line into the L2 cache initiated from the core. This includes stash requests to lines that are already in the L2 cache. If the cluster does not contain an L2 cache, this event does not count as the prefetcher is implicitly disabled.
0x00C2	0x-	L1D_CACHE_REFILL_PREFETCH	L1 data cache refill due to prefetch. Counts any linefills from the prefetcher which cause an allocation into the L1 D-cache.
0x00C3	0x-	L2D_WS_MODE	L2 cache write streaming mode. Counts for each cycle where the core is in write-streaming mode and not allocating writes into the L2 cache.
0x00C4	0x-	L1D_WS_MODE_ENTRY	L1 data cache entering write streaming mode. Counts for each entry into write-streaming mode.
0x00C5	0x-	L1D_WS_MODE	L1 data cache write streaming mode. Counts for each cycle where the core is in write-streaming mode and not allocating writes into the L1 D-cache.
0x00C9	0x-	BR_COND_PRED	Predicted conditional branch executed. Counts when any branch which can be predicted by the conditional predictor is retired. This event still counts when branch prediction is disabled due to the MMU being off.

Event code	ETM code	Mnemonic	Description
0x00CA	0x-	BR_INDIRECT_MIS_PRED	Indirect branch mis-predicted. Counts when any indirect branch which can be predicted by the BTAC is retired, and has mis-predicted for either the condition or the address. This event still counts when branch prediction is disabled due to the MMU being off.
0x00CB	0x-	BR_INDIRECT_ADDR_MIS_PRED	Indirect branch mis-predicted due to address mis-compare. Counts when any indirect branch which can be predicted by the BTAC is retired, was taken and correctly predicted the condition, and has mis-predicted the address. This event still counts when branch prediction is disabled due to the MMU being off.
0x00CC	0x-	BR_COND_MIS_PRED	Conditional branch mis-predicted. Counts when any branch which can be predicted by the conditional predictor is retired, and has mis-predicted the condition. This event still counts when branch prediction is disabled due to the MMU being off. Conditional indirect branches which correctly predicted the condition but mis-predicted on the address do not count this event.
0x00CD	0x-	BR_INDIRECT_ADDR_PRED	Indirect branch with predicted address executed. Counts when any indirect branch which can be predicted by the BTAC is retired, was taken and correctly predicted the condition. This event still counts when branch prediction is disabled due to the MMU being off.
0x00CE	0x-	BR_RETURN_ADDR_PRED	Procedure return with predicted address executed. Counts when any procedure return which can be predicted by the CRS is retired, was taken and correctly predicted the condition. This event still counts when branch prediction is disabled due to the MMU being off.
0x00CF	0x-	BR_RETURN_ADDR_MIS_PRED	Procedure return mis-predicted due to address mis-compare. Counts when any procedure return which can be predicted by the CRS is retired, was taken and correctly predicted the condition, and has mis-predicted the address. This event still counts when branch prediction is disabled due to the MMU being off.
0x00D0	0x-	L2D_LLWALK_TLB	L2 TLB last-level walk cache access. This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x00D1	0x-	L2D_LLWALK_TLB_REFILL	L2 TLB last-level walk cache refill. This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x00D2	0x-	L2D_L2WALK_TLB	L2 TLB level-2 walk cache access. This event count accesses to the level-2 walk cache where the last-level walk cache has missed. The event only counts when the translation regime of the pagewalk uses level 2 descriptors. This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x00D3	0x-	L2D_L2WALK_TLB_REFILL	L2 TLB level-2 walk cache refill. This event does not count if the MMU is disabled. This event counts only when the MMU is present.
0x00E1	0x-	STALL_FRONTEND_CACHE	No operation issued due to the frontend, cache miss. Counts every cycle the DPU IQ is empty and there is an instruction cache miss being processed
0x00E2	0x-	STALL_FRONTEND_TLB	No operation issued due to the frontend, TLB miss. Counts every cycle the DPU IQ is empty and there is an instruction L1-TLB miss being processed
0x00E4	0x-	STALL_BACKEND_ILOCK	No operation issued due to the backend, interlock. Counts every cycle that issue is stalled due to a dependency. Stall cycles due to a stall in Wr (typically awaiting load data) are excluded.
0x00E5	0x-	STALL_BACKEND_ILOCK_AGU	No operation issued due to the backend, interlock, AGU. Counts every cycle that issue is stalled due to a load/store instruction waiting for data to calculate the address in the AGU. Stall cycles due to a stall in Wr (typically awaiting load data) are excluded.

Event code	ETM code	Mnemonic	Description
0x00E6	0x-	STALL_BACKEND_ILOCK_FPU	No operation issued due to the backend, interlock, FPU. Counts every cycle that issue is stalled due to a dependency of an FPU/NEON instruction. Stall cycles due to a stall in the Wr stage (typically awaiting load data) are excluded.
0x00E7	0x-	STALL_BACKEND_LD	No operation issued due to the backend, load. Counts every cycle there is a stall in the Wr stage due to a load.
0x00E8	0x-	STALL_BACKEND_ST	No operation issued due to the backend, store. Counts every cycle there is a stall in the Wr stage due to a store.
0x00E9	0x-	STALL_BACKEND_LD_CACHE	No operation issued due to the backend, load, cache miss. Counts every cycle there is a stall in the Wr stage due to a load which is waiting on data (due to missing the cache or being non-cacheable).
0x00EA	0x-	STALL_BACKEND_LD_TLB	No operation issued due to the backend, load, TLB miss. Counts every cycle there is a stall in the Wr stage due to a load which has missed in the L1 TLB.
0x00EB	0x-	STALL_BACKEND_ST_STB	No operation issued due to the backend, store, STB full. Counts every cycle there is a stall in the Wr stage due to a store which is waiting due to the STB being full.
0x00EC	0x-	STALL_BACKEND_ST_TLB	No operation issued due to the backend, store, TLB miss. Counts every cycle there is a stall in the Wr stage due to a store which has missed in the L1 TLB.
0x00ED	0x-	STALL_BACKEND_LD_RAW	No operation issued due to the backend, load, stalled due to a read-after-write hazard.
0x0300	0x-	BR_NANO_IMM_ACCESS	Fetch pipeline accessed nano predictors for an immediate branch.
0x0301	0x-	BR_NANO_IMM_HIT	An immediate branch hit in the nano predictors in the fetch pipeline.
0x0302	0x-	BR_NANO_IMM_MIS_PRED	An immediate branch mis-predicted in the nano predictors in the fetch pipeline.
0x0304	0x-	BR_NANO_COND_ACCESS	Fetch pipeline accessed nano predictors for a conditional branch.
0x0305	0x-	BR_NANO_COND_HIT	A conditional branch hit in the nano predictors in the fetch pipeline.
0x0306	0x-	BR_NANO_COND_MIS_PRED	A conditional branch mis-predicted in the nano predictors in the fetch pipeline.
0x0307	0x-	BR_NANO_INDIRECT_ACCESS	Fetch pipeline accessed nano predictors for an indirect branch.
0x0308	0x-	BR_NANO_INDIRECT_HIT	An indirect branch hit in the nano predictors in the fetch pipeline.
0x0309	0x-	BR_NANO_INDIRECT_MIS_PRED	An indirect branch mis-predicted in the nano predictors in the fetch pipeline.
0x030a	0x-	BR_NANO_RETURN_ACCESS	Fetch pipeline accessed nano predictors for a return instruction.
0x030b	0x-	BR_NANO_RETURN_HIT	A return instruction hit in the nano predictors in the fetch pipeline.
0x030c	0x-	BR_NANO_RETURN_MIS_PRED	A return instruction mis-predicted in the nano predictors in the fetch pipeline.
0x030d	0x-	MM_L1I_PREFETCH_ACCESS	This event counts accesses to L1 Icache initiated by the prefetcher to an address mapped to the main manager port.
0x030e	0x-	MM_L1I_PREFETCH_REFILL	This event counts Icache refills initiated by the prefetcher to an address mapped to the main manager port.
0x030f	0x-	LLRAM_L1I_PREFETCH_ACCESS	This event counts accesses to L1 Icache initiated by the prefetcher to an address mapped to the LLRAM port.
0x0310	0x-	LLRAM_L1I_PREFETCH_REFILL	This event counts Icache refills initiated by the prefetcher to an address mapped to the LLRAM port.
0x0320	0x-	SYS_CACHE_RD	This event counts any cacheable read transaction which returns a data source of interconnect cache or inter-cluster peer.



Event code	ETM code	Mnemonic	Description
0x0321	0x-	SYS_CACHE_MISS_RD	This event counts any cacheable read transaction which returns a data source of DRAM.
0x0322	0x-	LLPP_ACCESS_RD	LLPP access, read, counts for every unique read request sent to the LLPP read address channel.
0x0323	0x-	LLPP_ACCESS_WR	LLPP access, write, counts for every unique write request sent to the LLPP write address channel.
0x0324	0x-	LLPP_ACCESS	Counts accesses made on the LLPP. This event is a sum of LLPP_ACCESS_WR and LLPP_ACCESS_RD.
0x0325	0x-	MM_ACCESS_RD	Bus access, read, Counts for every beat of data transferred over the read data channel between the shared L2 and the core.
0x0326	0x-	MM_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the core and the L2.
0x0327	0x-	MM_ACCESS	Counts accesses made on the main manager channel between the core and the L2. This event is a sum of MM_ACCESS_WR and MM_ACCESS_RD.
0x0328	0x-	LLRAM_ACCESS_RD	Bus access, read, Counts for every beat of data transferred over the read data channel between the LLRAM coherency unit and the core targetting the LLRAM port.
0x0329	0x-	LLRAM_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the core and LLRAM coherency unit targetting the LLRAM port.
0x032a	0x-	LLRAM_ACCESS	Counts accesses made between the core and the LLRAM coherency unit targetting the LLRAM port. This event is a sum of LLRAM_ACCESS_WR and LLRAM_ACCESS_RD.
0x032b	0x-	SPP_ACCESS_RD	Bus access, read, Counts for every beat of data transferred over the read data channel between the LLRAM coherency unit and the core targetting the SPP port.
0x032c	0x-	SPP_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the core and LLRAM coherency unit targetting the SPP port.
0x032d	0x-	SPP_ACCESS	Counts accesses made between the core and the LLRAM coherency unit targetting the SPP port. This event is a sum of SPP_ACCESS_WR and SPP_ACCESS_RD.
0x032e	0x-	LLPP_CYCLES	Low latency peripheral port bus has outstanding transactions (counted on SCLK instead of bus clock)
0x032f	0x-	LLPP_ACTIVE	Low latency peripheral port cycles
0x0330	0x-	TCMS_ACCESS_RD	ACELS access to TCMs, read, counts for every unique read request sent to the TCMs from the ACELS port to this core.
0x0331	0x-	TCMS_ACCESS_WR	ACELS access to TCMs, write, counts for every unique write request sent to the TCMs from the ACELS port to this core.
0x0332	0x1A	TCMS_ACCESS	Counts accesses made between the ACELS port and the core. This event is a sum of TCMS_ACCESS_WR and TCMS_ACCESS_RD.
0x0333	0x18	TCMS_CONTENTION	Counts every stall cycle due to contention of accessing ITCM and DTCM via the ACELS port at the same time.
0x0334	0x-	MM_SNP_ACCESS	Counts every unique snoop request received by the core from the L2. This includes snoops received from the own core, another core or from outside the cluster in the CHI configuration.

Event code	ETM code	Mnemonic	Description
0x0335	0x-	LLRAM_SNP_ACCESS	Counts every unique snoop request received by the core from the LLRAM coherency unit. This includes snoops received from the own core or another core.
0x0336	0x-	SNP_ACCESS	Counts every unique snoop request received by the core. This event is a sum of MM_SNP_ACCESS and LLRAM_SNP_ACCESS.
0x0337	0x-	MM_SNP_ACCESS_EVICT	Counts every unique snoop request received by the core from the L2 that evicts data. This includes snoops received from the own core, another core or from outside the cluster in the CHI configuration.
0x0338	0x-	LLRAM_SILENT_EVICT	Counts every instance of silently evicting a valid LLRAM line in the L1D cache in order to allocate a main manager address in the same set/way.
0x0339	0x-	TCMS_SERIALISATION_CONTENTION	Counts every stall cycle due to contention of read and write channel requesting serialization at the same time.
0x0340	0x-	LLRAM_SNP_ACCESS_EVICT	Counts every unique snoop request received by the core from the LCU that evicts data. This includes only snoops received from the own core.
0x0350	0x-	MM_L1I_CACHE_REFILL	L1 instruction cache refill for an address to the Main Manager (MM) region. Counts any instruction fetch which misses in the cache and starts a new cache refill. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted.
0x0351	0x-	MM_L1I_CACHE	L1 instruction cache access targeting the main manager port.
0x0352	0x-	MM_L1D_CACHE_REFILL_RD	L1 data cache refill, read from the main manager port.
0x0353	0x-	MM_L1D_CACHE_REFILL_WR	L1 data cache refill, write from the main manager port.
0x0354	0x-	MM_L1D_CACHE_REFILL	L1 data cache refill for the main manager port. This event counts the sum of MM_L1D_CACHE_REFILL_RD and MM_L1D_CACHE_REFILL_WR.
0x0355	0x-	MM_L1D_CACHE_RD	L1 data cache access, read targeting the main manager address region.
0x0356	0x-	MM_L1D_CACHE_WR	L1 data cache access, write targeting the main manager address region.
0x0357	0x-	MM_L1D_CACHE	L1 data cache access targeting the main manager port. This event counts the sum of MM_L1D_CACHE_RD and MM_L1D_CACHE_WR.
0x0358	0x-	LLRAM_L1I_CACHE_REFILL	L1 instruction cache refill for an address to the Low-latency RAM (LLRAM) region. Counts any instruction fetch which misses in the cache and starts a new cache refill. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted.
0x0359	0x-	LLRAM_L1I_CACHE	L1 instruction cache access targeting the Low-latency RAM (LLRAM) region.
0x0360	0x-	LLRAM_L1D_CACHE_REFILL_RD	L1 data cache refill, read from the LLRAM port.
0x0361	0x-	LLRAM_L1D_CACHE_REFILL_WR	L1 data cache refill, write from the LLRAM port.
0x0362	0x-	LLRAM_L1D_CACHE_REFILL	L1 data cache refill from the LLRAM port. This event counts the sum of LLRAM_L1D_CACHE_REFILL_RD and LLRAM_L1D_CACHE_REFILL_WR.
0x0363	0x-	LLRAM_L1D_CACHE_RD	L1 data cache access, read targeting the LLRAM address region.
0x0364	0x-	LLRAM_L1D_CACHE_WR	L1 data cache access, write targeting the LLRAM address region.
0x0365	0x-	LLRAM_L1D_CACHE	L1 data cache access targeting the LLRAM address region. This event counts the sum of LLRAM_L1D_CACHE_RD and LLRAM_L1D_CACHE_WR.
0x0366	0x-	LLRAM_L1D_CACHE_REFILL_MERGED	L1 data cache refill from the LLRAM port merged with a previous ongoing refill to the same cacheline address.
0x0367	0x-	LLRAM_L1D_CACHE_REFILL_FAIL	L1 data cache refill from the LLRAM port failed to allocate into the cache.

Event code	ETM code	Mnemonic	Description
0x0368	0x-	LLRAM_L1D_CACHE_REFILL_MM_EVICT	L1 data cache refill from the LLRAM port first requires a main manager line to be evicted from the cache. This event counts the request sent to L2 to evict the MM line from L1D cache.
0x0369	0x-	MM_L1D_CACHE_REFILL_MERGED	L1 data cache refill from the main manager port merged with a previous ongoing refill to the same cacheline address.
0x0370	0x-	TCM_ACCESS_D_RD	I or D TCM accessed from the data side for a read operation.
0x0371	0x-	TCM_ACCESS_D_WR	I or D TCM accessed from the data side for a write operation.
0x0372	0x-	TCM_ACCESS_I	ITCM accessed from the instruction pipe.
0x0373	0x-	ROUTER_STALL	More than one router packet needs arbitrating introducing contention.
0x0374	0x-	MM_STB_FULL	Counts every time the main manager STB slots are full.
0x0375	0x-	LLRAM_STB_FULL	Counts every time the LLRAM STB slots are full. This event also covers accesses to the SPP region.
0x0376	0x-	LLPP_STB_FULL	Counts every time the LLPP STB slots are full.
0x0377	0x-	TCMS_STB_FULL	Counts every time the TC STB slots are full.
0x0378	0x-	BARRIER_STB_FULL	Counts every time the barrier STB slots are full.
0x0379	0x-	L1I_WT_HIT	L1 Instruction cache way tracker hit
0x037a	0x-	L1D_WT_HIT_RD	L1 Data cache way tracker hit for a read operation from the data cache.
0x037b	0x-	L1D_WT_HIT_WR	A lookup into the TLAC hit.
0x0390	0x29	VSCTLR_WR_RETIRED	Instruction architecturally executed, condition code check pass, write to VSCTLR_EL2.
0x0391	0x28	DFB_RETIRED	Instruction architecturally executed, condition code check pass for data full barrier instruction.
0x0392	0x27	EL2_ENTERED	Exception taken to EL2 (hyp mode entry), excluding reset
0x0395	0x35	LLRAM_TIMEOUT	An event to indicate that a transaction has timed out on an access to the LLRAM region
0x0396	0x36	MM_TIMEOUT	An event to indicate that a transaction has timed out on an access to the main manager region
0x0397	0x34	LLPP_TIMEOUT	An event to indicate that a transaction has timed out on an access to the LLPP region
0x0398	0x37	SPP_TIMEOUT	An event to indicate that a transaction has timed out on an access to the SPP region
0x0399	0x-	L1D_TLB_REFILL_PREFETCHER	L1 TLB refill used by the data side prefetcher. Counts any refill of the data L1-MMS from the L2 MMS. This includes refills which result in a translation fault. This event counts regardless of whether translation is enabled.
0x039a	0x-	L1D_TLB_PREFETCHER	L1 TLB access by the data side prefetcher.

#### 14.4.1.4 Recommended implementation defined core PMU events

Arm recommends some implementation defined core PMU events.

The following table shows the recommended implementation defined events that are generated at the core and the numbers that the *Performance Monitoring Unit* (PMU) in that core uses to reference the events.

**Table 14-5: Recommended implementation defined core PMU events**

Event code	ETM code	Mnemonic	Description
0x0040	0x-	L1D_CACHE_RD	L1 data cache access, read. Counts any load operation or pagewalk access which looks up in the L1 data cache. In particular, any access which could count the L1D_CACHE_REFILL_RD event causes this event to count. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted.
0x0041	0x-	L1D_CACHE_WR	L1 data cache access, write. Counts any store operation which looks up in the L1 data cache. In particular, any access which could count the L1D_CACHE_REFILL_WR event causes this event to count. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted. This event is a sum of MM_L1D_CACHE_WR and LLRAM_L1D_CACHE_WR.
0x0042	0x-	L1D_CACHE_REFILL_RD	L1 data cache refill, read. Counts any load operation or pagewalk access which causes data to be read from outside the L1, including accesses which do not allocate into L1. Cache maintenance instructions and prefetches are not counted. Non-cacheable accesses are not counted. This event is a sum of MM_L1D_CACHE_REFILL_RD and LLRAM_L1D_CACHE_REFILL_RD.
0x0043	0x-	L1D_CACHE_REFILL_WR	L1 data cache refill, write. Counts any store operation which causes data to be read from outside the L1, including accesses which do not allocate into L1. Cache maintenance instructions and prefetches are not counted. Stores of an entire cache line are not counted, even if they make a coherency request outside the L1. Partial cache line writes which do not allocate into the L1 cache are not counted. Non-cacheable accesses are not counted. This event is a sum of MM_L1D_CACHE_REFILL_WR and LLRAM_L1D_CACHE_REFILL_WR.
0x0044	0x-	L1D_CACHE_REFILL_INNER	L1 data cache refill, inner main manager address. Counts any L1 D-cache linefill (as counted by L1D_CACHE_REFILL) which hits in the L2 cache, or another core in the cluster.
0x0045	0x-	L1D_CACHE_REFILL_OUTER	L1 data cache refill, outer main manager address. Counts any L1 D-cache linefill (as counted by L1D_CACHE_REFILL) which does not hit in the L2 cache, or another core in the cluster, and instead obtains data from outside the cluster.
0x0050	0x-	L2D_CACHE_RD	L2 cache access, read, main manager address. This event counts any cacheable read transaction which returns a data source of local cluster or peer CPU.
0x0060	0x-	BUS_ACCESS_RD	Bus access, read. Counts for every beat of data transferred over the read data channel between the core and the SCU. This event is a sum of LLPP_ACCESS_RD, MM_ACCESS_RD, LLRAM_ACCESS_RD, SPP_ACCESS_RD and TCMS_ACCESS_RD.
0x0061	0x-	BUS_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the core and the SCU. This event is a sum of LLPP_ACCESS_WR, MM_ACCESS_WR, LLRAM_ACCESS_WR, SPP_ACCESS_WR and TCMS_ACCESS_WR.
0x0066	0x-	MEM_ACCESS_RD	Data memory access, read. Counts memory accesses due to load instructions. Does not count instruction fetches, cache maintenance instructions, translation table walks or prefetches.
0x0067	0x-	MEM_ACCESS_WR	Data memory access, write. Counts memory accesses due to store instructions. Does not count instruction fetches, cache maintenance instructions, translation table walks or prefetches.
0x0070	0x-	LD_SPEC	Operation speculatively executed, load.
0x0071	0x-	ST_SPEC	Operation speculatively executed, store.
0x0072	0x-	LDST_SPEC	Operation speculatively executed, load or store. This event counts the sum of LD_SPEC and ST_SPEC.
0x0073	0x-	DP_SPEC	Operation speculatively executed, integer data-processing.
0x0074	0x-	ASE_SPEC	Operation speculatively executed, Advanced SIMD instruction.

Event code	ETM code	Mnemonic	Description
0x0075	0x-	VFP_SPEC	Operation speculatively executed, floating-point instruction.
0x0076	0x-	PC_WRITE_SPEC	Operation speculatively executed, software change of the Program Counter.
0x0078	0x-	BR_IMMED_SPEC	Branch speculatively executed, immediate branch.
0x0079	0x-	BR_RETURN_SPEC	Branch speculatively executed, procedure return.
0x007A	0x-	BR_INDIRECT_SPEC	Branch speculatively executed, indirect branch.
0x0082	0x33	EXC_SVC	Exception taken, supervisor call
0x0086	0x32	EXC_IRQ	Exception taken, IRQ
0x0087	0x31	EXC_FIQ	Exception taken, FIQ
0x008A	0x30	EXC_HVC	Exception taken, Hypervisor Call
0x008E	0x2F	EXC_TRAP_IRQ	Exception taken, IRQ not taken locally
0x008F	0x2E	EXC_TRAP_FIQ	Exception taken, FIQ not taken locally

## 14.4.2 Cluster PMU events

The cluster *Performance Monitoring Unit* (PMU) collects events from the shared units and use event codes to reference these events. Cluster PMU events are implementation defined.

### 14.4.2.1 Implementation defined cluster PMU events

The following table shows the implementation defined events that are generated at the cluster and the numbers that the *Performance Monitoring Unit* (PMU) uses to reference the events.

**Table 14-6: Implementation defined cluster PMU events**

Event code	ETM code	Mnemonic	Description
0x0419	0x-	MM_ACCESS	Main Manager bus access counter. This event is a sum of MM_ACCESS_RD and MM_ACCESS_WR.
0x041A	0x-	MM_ACTIVE	Main Manager bus has outstanding transactions (counted on SCLK instead of bus clock)
0x041D	0x-	MM_CYCLES	Main Manager bus cycles
0x0460	0x-	MM_ACCESS_RD	Main Manager access, read. Counts for every beat of data transferred over the read data channel between the cluster and the interconnect.
0x0461	0x-	MM_ACCESS_WR	Main Manager access, write. Counts for every beat of data transferred over the write data channel between the cluster and the interconnect.
0x0462	0x-	MM_ACCESS_SHARED	Main Manager access, shared. Counts for every beat of shared data transferred over the data channels between the cluster and the interconnect.
0x0463	0x-	MM_ACCESS_NOT_SHARED	Main Manager access, not shared. Counts for every beat of not shared data transferred over the data channels between the cluster and the interconnect.
0x0464	0x-	MM_ACCESS_NORMAL	Main Manager access, normal. Counts for every beat of normal data transferred over the data channels between the cluster and the interconnect.
0x0465	0x-	MM_ACCESS_PERIPH	Main Manager access, periph. Counts for every beat of device data transferred over the data channels between the cluster and the interconnect.

Event code	ETM code	Mnemonic	Description
0x0466	0x-	MM_CHI_SNP_ACCESS	L2 external snoop access counter. Counts every external snoop request.
0x0467	0x-	MM_CHI_SNP_EVICT	L2 external snoop eviction counter. Counts every external snoop request that causes an L2 cache eviction.
0x0468	0x-	MM_CHI_SNP_NO_CPU	L2 external No-cpu snoop access counter. Counts every external snoop request that completes without snooping a core.
0x0469	0x-	MM_PREFETCH_CPU_ACCESS	L2 prefetch access, CPU counter. Counts every stash transaction originating from a core.
0x0470	0x-	MM_PREFETCH_CPU_HIT	L2 prefetch data hit, CPU counter. Counts every stash transaction originating from a core where the stash hit in the cluster.
0x0471	0x-	MM_PREFETCH_CPU_MISS	L2 prefetch data miss, CPU counter. Counts every stash transaction originating from a core where data was read in from outside the cluster.
0x0472	0x-	MM_PREFETCH_CPU_MATCH	L2 prefetch matching access, CPU counter. Counts every completed stash transaction originating from a core that is matched by a compatible read request.
0x0473	0x-	MM_PREFETCH_CPU_KILL	L2 prefetch terminated access, CPU counter. Counts every stash transaction originating from a core that is terminated due to an incompatible match.
0x0474	0x-	MM_CHI_STASH_ICN_ACCESS	L2 stash access, ICN counter. Counts every stash transaction originating from the interconnect.
0x0475	0x-	MM_CHI_STASH_ICN_HIT	L2 stash data hit, ICN counter. Counts every stash transaction originating from the interconnect where the stash hit in the cluster.
0x0476	0x-	MM_CHI_STASH_ICN_MISS	L2 stash data miss, ICN counter. Counts every stash transaction originating from the interconnect where data was read in from outside the cluster.
0x0477	0x-	MM_CHI_STASH_ICN_MATCH	L2 stash matching access, ICN counter. Counts every completed stash transaction originating from the interconnect that is matched by a compatible read request.
0x0478	0x-	MM_CHI_STASH_ICN_KILL	L2 stash terminated access, ICN counter. Counts every stash transaction originating from the interconnect that is terminated due to an incompatible match.
0x0484	0x-	MM_HAZARD_ADDR	L2 address hazard. Request flushed and replayed due to address match with earlier request.
0x0485	0x-	MM_HAZARD_L2DB	L2 data buffer hazard. Request flushed and replayed due to L2DBs not available.
0x0486	0x-	MM_HAZARD_AFB	L2 address forwarding buffer hazard. Request flushed and replayed due to AFB not available.
0x0487	0x-	MM_HAZARD_STU_DRAIN	L2 STU drain hazard. Read after Write hazard or Data Buffers full requiring force drain of the STU.
0x0488	0x-	MM_MEMORY_ERROR	Local memory error. Counts any Correctable or Uncorrectable memory error (ECC or parity) in the Duplicate Tags, L2 Tag or Data and L2DBs.
0x0119	0x-	MACP_ACCESS	Main Accelerator Coherency Port (MACP) bus access counter. This event is a sum of MACP_ACCESS_RD and MACP_ACCESS_WR.
0x011A	0x-	MACP_ACTIVE	MACP bus has outstanding transactions (counted on SCLK instead of bus clock)
0x011D	0x-	MACP_CYCLES	MACP bus cycles
0x0160	0x-	MACP_ACCESS_RD	MACP bus read access counter. Counts for every beat transferred over the read data channel between the interconnect and the cluster.
0x0161	0x-	MACP_ACCESS_WR	MACP bus write access counter. Counts for every beat transferred over the write data channel between the interconnect and the cluster.
0x0162	0x-	MACP_STASH_ACP_ACCESS	L2 stash access, ACP counter. Counts every stash transaction originating from the MACP.

Event code	ETM code	Mnemonic	Description
0x0163	0x-	MACP_STASH_ACP_HIT	L2 stash data hit, ACP counter. Counts every stash transaction originating from the MACP where the stash hit in the cluster.
0x0164	0x-	MACP_STASH_ACP_MISS	L2 stash data miss, ACP counter. Counts every stash transaction originating from the MACP where data was read in from outside the cluster.
0x0165	0x-	MACP_STASH_ACP_MATCH	L2 stash matching access, ACP counter. Counts every completed stash transaction originating from the MACP that is matched by a compatible read request.
0x0166	0x-	MACP_STASH_ACP_KILL	L2 stash terminated access, ACP counter. Counts every stash transaction originating from the MACP that is terminated due to an incompatible match.
0x0319	0x-	ACELS_ACCESS	ACE-Lite Subordinate (ACELS) bus access counter. This event is a sum of ACELS_ACCESS_RD and ACELS_ACCESS_WR.
0x031D	0x-	ACELS_CYCLES	ACELS bus cycles
0x0360	0x-	ACELS_ACCESS_RD	ACELS bus read access counter. This event counts accesses on the read address channel.
0x0361	0x-	ACELS_ACCESS_WR	ACELS bus write access counter. This event counts accesses on the write address channel.
0x0362	0x-	ACELS_HAZARD_ID_RD	ACELS request stalled due to ID hazard on the read address channel
0x0363	0x-	ACELS_HAZARD_ID_WR	ACELS request stalled due to ID hazard on the write address channel.
0x0364	0x-	ACELS_HAZARD_RESP_RD	ACELS response on the read channel delayed due to arbitration contention.
0x0365	0x-	ACELS_HAZARD_RESP_WR	ACELS response on the write channel delayed due to arbitration contention.
0x0219	0x-	SPP_ACCESS	Shared Peripheral Port bus access counter. This event is a sum of SPP_ACCESS_RD and SPP_ACCESS_WR.
0x021A	0x-	SPP_ACTIVE	Shared Peripheral Port bus has outstanding transactions (counted on SCLK instead of bus clock).
0x021D	0x-	SPP_CYCLES	Shared Peripheral Port cycles
0x0260	0x-	SPP_ACCESS_RD	Shared Peripheral Port access, read. Counts for every beat of data transferred over the read data channel on the port.
0x0261	0x-	SPP_ACCESS_WR	Shared Peripheral Port access, write. Counts for every beat of data transferred over the write data channel on the port.
0x0519	0x-	L2_CACHE	L2 unified cache access counter. Counts every cacheable read or write transaction issued to the L2. This event is a sum of L2_CACHE_RD and L2_CACHE_WR.
0x0520	0x-	L2_CACHE_RD	L2 unified cache access, read counter. Counts every cacheable read transaction issued to the L2 (excluding prefetches and stashes).
0x0521	0x-	L2_CACHE_WR	L2 unified cache access, write counter. Counts every cacheable write transaction issued to the L2.
0x0522	0x-	L2_CACHE_REFILL	L2 unified cache access refill counter. Counts every cacheable read or write transaction issued to the interconnect. This event is a sum of L2_CACHE_REFILL_RD and L2_CACHE_REFILL_WR.
0x0523	0x-	L2_CACHE_REFILL_RD	L2 unified cache access, read refill counter. Counts every cacheable read transaction issued to the interconnect (excluding prefetches and stashes).
0x0524	0x-	L2_CACHE_REFILL_WR	L2 unified cache access, write refill counter. Counts every cacheable write transaction issued to the interconnect.
0x0525	0x-	L2_CACHE_WB	L2 unified cache writeback counter. Counts every write-back from the L2 cache.
0x0526	0x-	L2_CACHE_ALLOCATE	L2 unified cache allocation without refill counter. Counts every full cache line write into the L2 cache which does not cause a linefill.

Event code	ETM code	Mnemonic	Description
0x0719	0x-	LLRAM_ACCESS	Low-latency RAM (LLRAM) bus access counter. This event is a sum of LLRAM_ACCESS_RD and LLRAM_ACCESS_WR.
0x071A	0x-	LLRAM_ACTIVE	LLRAM bus has outstanding transactions (counted on SCLK instead of bus clock).
0x071D	0x-	LLRAM_CYCLES	LLRAM bus cycles
0x0760	0x-	LLRAM_ACCESS_RD	Bus access, read. Counts for every beat of data transferred over the read data channel between the cluster and the interconnect.
0x0761	0x-	LLRAM_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the cluster and the interconnect.
0x0762	0x-	LLRAM_ACCESS_SHARED	Bus access, shared. Counts for every beat of shared data transferred over the data channels between the cluster and the interconnect.
0x0763	0x-	LLRAM_ACCESS_NOT_SHARED	Bus access, not shared. Counts for every beat of not shared data transferred over the data channels between the cluster and the interconnect.
0x0764	0x-	LLRAM_ACCESS_NORMAL	Bus access, normal. Counts for every beat of normal data transferred over the data channels between the cluster and the interconnect.
0x0765	0x-	LLRAM_ACCESS_PERIPH	Bus access, periph. Counts for every beat of device data transferred over the data channels between the cluster and the interconnect.
0x0766	0x-	LLRAM_HAZARD_ADDR	LCU address hazard. Request ordered due to address match with earlier request.
0x0767	0x-	LLRAM_HAZARD_SET_WAY	LCU set/way hazard. Request ordered due to set/way match with earlier request.
0x0768	0x-	LLRAM_HAZARD_STU_DRAIN	LCU STU drain hazard. Read after Write hazard or LCU Data Buffers full requiring LCU force drain of the STU.
0x0769	0x-	LLRAM_MEMORY_ERROR	Local memory error. Counts any Correctable or Uncorrectable memory error (ECC or parity) in the Duplicate Tags.
0x0819	0x-	ROUTER_STALL	More than one router packet needs arbitrating introducing contention.

#### 14.4.2.2 Recommended implementation defined cluster PMU events

Arm recommends some implementation defined PMU events at the cluster.

The following table shows the recommended implementation defined events that are generated at the cluster and the numbers that the *Performance Monitoring Unit* (PMU) uses to reference the events.

**Table 14-7: Recommended implementation defined cluster PMU events**

Event code	ETM code	Mnemonic	Description
0x0011	0x-	CYCLES	Clock cycles
0x0019	0x-	BUS_ACCESS	Bus access, read or write. Counts for every beat of data transferred over the read or write data channel between the cluster and the interconnect.
0x001A	0x-	MEMORY_ERROR	Local memory error. Counts any Correctable or Uncorrectable memory error (ECC or parity) in the protected RAMs.
0x001D	0x-	BUS_CYCLES	Bus clock cycle
0x001E	0x-	CHAIN	Odd performance counter chain mode



Event code	ETM code	Mnemonic	Description
0x0060	0x-	BUS_ACCESS_RD	Bus access, read. Counts for every beat of data transferred over the read data channel between the cluster and the interconnect.
0x0061	0x-	BUS_ACCESS_WR	Bus access, write. Counts for every beat of data transferred over the write data channel between the cluster and the interconnect.
0x0062	0x-	BUS_ACCESS_SHARED	Bus access, shared. Counts for every beat of shared data transferred over the data channels between the cluster and the interconnect.
0x0063	0x-	BUS_ACCESS_NOT_SHARED	Bus access, not shared. Counts for every beat of not shared data transferred over the data channels between the cluster and the interconnect.
0x0064	0x-	BUS_ACCESS_NORMAL	Bus access, normal. Counts for every beat of normal data transferred over the data channels between the cluster and the interconnect.
0x0065	0x-	BUS_ACCESS_PERIPH	Bus access, periph. Counts for every beat of device data transferred over the data channels between the cluster and the interconnect.

## 14.5 PMU interrupts

The Cortex®-R82AE processor asserts nCLUSTERPMUIRQ and nPMUIRQ signals when the PMU generates an interrupt.

The Cortex®-R82AE processor asserts:

- The nCLUSTERPMUIRQ signal when the cluster PMU generates an interrupt.
- The nPMUIRQ[k] signal where k is the core ID, when the per-core PMU generates an interrupt.

You can route nCLUSTERPMUIRQ and nPMUIRQ signals to an external interrupt controller for prioritization and masking. This is the only mechanism that signals these interrupts to a core. nCLUSTERPMUIRQ and nPMUIRQ interrupts are also driven as a trigger input to the cluster *Cross Trigger Interface* (CTI) and core CTI respectively.

## 14.6 PMU register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor AArch64 Performance Monitors registers in [A.1.3 AArch64 Performance Monitors registers summary](#) on page 313.

You can find the register summary table for the core external Performance Monitors registers in [B.2.1.8 External PMU registers summary](#) on page 1721 and cluster external Performance Monitors registers in [B.2.1.2 External CLUSTERPMU registers summary](#) on page 1710.

# 15. ETM

This chapter describes the *Embedded Trace Macrocell* (ETM) for the Cortex®-R82AE processor.

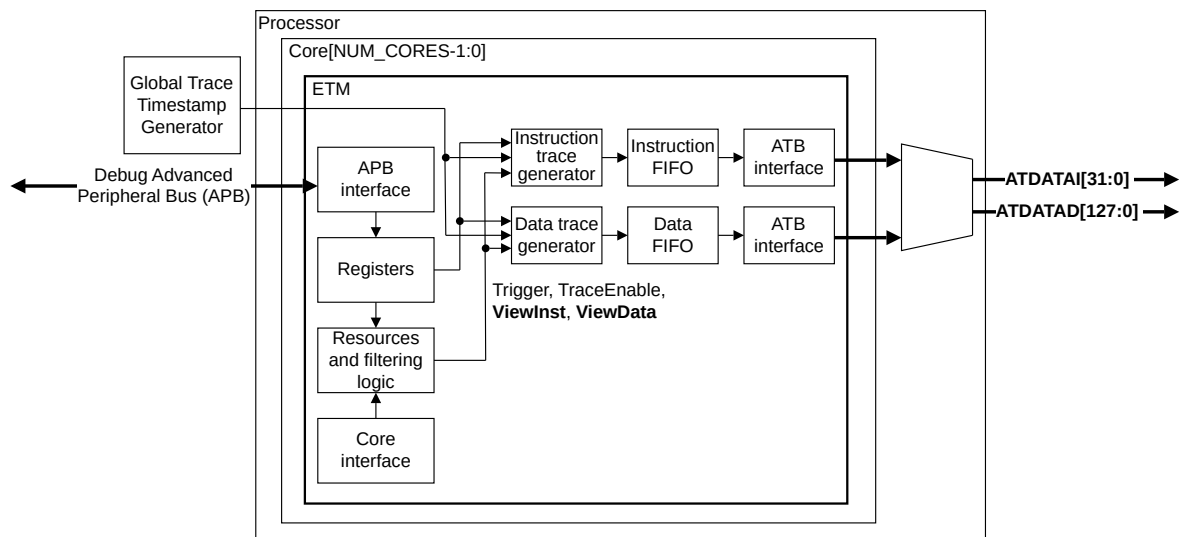
## 15.1 About the ETM

The *Embedded Trace Macrocell* (ETM) performs real-time instruction and data flow tracing based on the ETM architecture ETMv4.5. The Cortex®-R82AE processor supports one ETM per core.

The ETM is a CoreSight™ component and is an integral part of the Arm Real-time Debug solution, DS-5 Development Studio. It enables non-invasive debugging of software running on one or more cores of the Cortex®-R82AE processor.

The following figure shows the main functional blocks of the ETM.

**Figure 15-1: ETM block diagram**



### Core interface

This block connects to the core within the Cortex®-R82AE processor. It tracks the execution information from the core, decodes the control signals, and passes on the information to the internal interfaces.

### Instruction trace generator

This block generates the trace packets which are a compressed form of the instruction execution information provided by the core. The trace packets are then passed to the instruction FIFO.

Data trace generator

This block generates the trace packets which are a compressed form of the data transfers (data address and data value) provided by the core. The trace packets are then passed to the data FIFO.

FIFO

This block buffers bursts of trace packets. Separate FIFOs are provided, one for the instruction trace stream, and one for the data trace stream.

Resources and filtering logic

These blocks contain resources which the trace software programs to trigger and filter the trace information. They start and stop trace generation, depending on the conditions that have been set.

ATB interfaces

There are two ATB interfaces:

- *Instruction ATB interface:* This reads up to four bytes of compressed packet information from the instruction FIFO and sends them over the instruction ATB interface. All the core ETM instruction trace streams are funneled into a single 32-bit ATB trace bus.
- *Data ATB interface:* This reads up to eight bytes of compressed packet information from the data FIFO and sends them over the data ATB interface. All the core ETM data trace streams and all the ELA trace streams are funneled into a single 128-bit ATB trace bus.

APB interface

This block implements the interface to the APB that provides access to the programmable registers.

Global timestamping

The ETM reuses the generic timer CNTVALUEB as a reference for timestamp packets.

This provides a 64-bit timestamp that a debugger can use for coarse-grained profiling, and correlation of trade sources.



Decompression of data trace relies on the presence of a global timestamp count.

15.2 ETM trace unit generation options and resources

The following table shows the resources of the ETM that are implemented.

Table 15-1: ETM trace unit resources implemented

Feature	Instance
Address comparators	4 pairs
Data value comparators	2

Feature	Instance
Context ID comparators	1
Virtual machine ID comparators	1
Single-Shot comparator resource	2
Counters	2
Cycle count size	12 bits
Number of sequencer states	4
Processor comparator inputs	0
External inputs	58
External outputs	4
External input selectors	4
Resource selector pairs	8
Instruction trace port size	32-bit
Data trace port size	64-bit
Instruction FIFO <sup>6</sup>	128 bytes with 32-bit output
Data FIFO	256 bytes with 64-bit output
Claim tag bits	4

The following table shows the optional features of the ETM architecture that the ETM implements.

**Table 15-2: ETM trace unit generation options implemented**

Feature	Implemented
Trace Start/Stop block	Yes
Trace all branches option	Yes
Trace of conditional instructions	Yes
Cycle counting in instruction trace	Yes
Data trace supported	Yes
Data address comparison	Yes
OS Lock mechanism	Yes
Secure non-invasive debug	Yes
Context ID tracing	Yes
Trace output	Yes
Timestamp size	64-bit
Memory mapped access to ETM registers	No
External debugger access to ETM registers	Yes
System instruction access to ETM registers	Yes
VMID comparator support	Yes
ATB trigger support	Yes

<sup>6</sup> Instruction trace can be configured to take priority over data trace. See bit[10] of the TRCSTALLCTLR.

## 15.3 ETM event connectivity

This section describes how the Cortex®-R82AE processor *Embedded Trace Macrocell* (ETM) inputs and outputs are connected to the *Cross Trigger Interface* (CTI) and *Performance Monitoring Unit* (PMU).

The following table shows the connection of the ETM external inputs that come from the CTI and PMU.

**Table 15-3: ETM External Input connections**

Bits	Description
ETM External Input 0	CTI Trigger Output 4
ETM External Input 1	CTI Trigger Output 5
ETM External Input 2	CTI Trigger Output 6
ETM External Input 3	CTI Trigger Output 7

The ETM external output resources are connected to the CTI, as the following table shows.

**Table 15-4: ETM External Output connections to CTI**

ETM output	CTI input
ETM External Output 0	CTI Trigger Input 4
ETM External Output 1	CTI Trigger Input 5
ETM External Output 2	CTI Trigger Input 6
ETM External Output 3	CTI Trigger Input 7

## 15.4 Operation

This section describes the R82AE processor *Embedded Trace Macrocell* (ETM) **IMPLEMENTATION DEFINED** features.

See the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#) for more information on the operation.

### 15.4.1 Precise TraceEnable events

The ViewInst and ViewData are imprecise under certain conditions, with some implementation-defined exceptions. The only condition which ensures that ViewInst and ViewData are precise is that the enabling event condition is TRUE.

For more information, see the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#).

### 15.4.2 Parallel instruction execution

The Cortex®-R82AE processor supports parallel instruction execution. The macrocell can trace up to three instructions per cycle and up to 256 bits of data transfer per cycle.

If ViewInst is active for a cycle, the ETM:

- Always traces all instructions reported to the ETM on the same cycle up to a branch if present.
- Any instructions from the previous cycle that follow a branch instruction.
- Can trace data for any of the instructions traced.

### 15.4.3 Comparator features

The ETM implements data address comparison. There are eight address comparators that can be configured for either instruction or data address comparison.

The ViewData instruction address comparators are sensitive to a batch of instructions which execute in consecutive cycles. If any instruction in the batch is in an include range and any instruction is not in an exclude range, then ViewData can be high.

See the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#) for a description of data address comparison.

### 15.4.4 Trace features

The ETM implements all of the ETMv4.5 trace features.

This means it supports:

- Data value and data address tracing.
- Data suppression.
- Cycle-accurate tracing.
- Timestamping.

See the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#) for a description of these features.

### 15.4.5 Packet formats

The Cortex®-R82AE processor ETM instruction trace interface does not support the following packet formats:

- Speculation resolution:

- Mispredict packet.
- Cancel format 2 and 3 packets.
- Conditional tracing:
  - All instruction format packets.
  - Result format 1 packet.
- Q packets.

The Cortex®-R82AE processor ETM data trace interface supports all data trace packet types except the P1 Format 6 and 7 packets.

See the [Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6](#) for the trace packet format descriptions.

### 15.4.6 Resource selection

The ETM uses event selectors to control resources.

The ETM controls the following resources:

- Trace events (triggers and markers in the trace stream).
- Timestamp event.
- ViewInst event.
- ViewData event.
- Counter control.
- Sequencer state transitions.

Each event selector is configured to be sensitive to a resource selector pair, and one resource selector pair can control more than one event selector.

The ETM provides one fixed resource selector pair, with static values of 0 and 1, and seven configurable selector pairs. A resource selector pair provides a bitfield OR selector for resources in two different groups, with each group and a configurable boolean combination provided.

The following shows the resources that can be selected for the instruction and data trace.

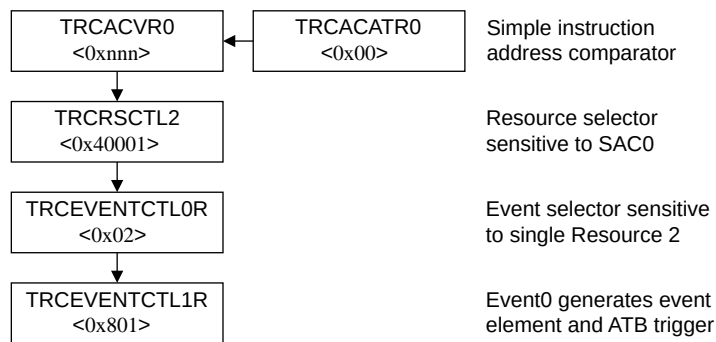
**Table 15-5: Instruction and data resource selection**

Group	Select	Resource
0b0000	0-3	External input selector 0-3
0b0010	0-1	Counter at zero 0-1
	4-7	Sequencer states 0-3
0b0011	1	Single-Shot comparator 0-1
0b0100	0-7	Single address comparator 0-7

Group	Select	Resource
0b0101	0-3	Address range comparator 0-3
0b0110	0	Context ID Comparator 0
0b0111	0	VMID Comparator 0

For example, the following figure shows the steps necessary to use a single address comparator to generate a trigger event and an ATB trigger. This example uses the first single resource selector that can be user-configured.

**Figure 15-2: Trigger event resource selection**



### 15.4.7 Trace flush behavior

Events that are observed by the ETM can be confirmed to have reached the trace bus output with the use of the ATB flush protocol. Both ATB ports must be flushed to determine when the trace infrastructure finishes capturing all the packets generated by the ETM.

ETM internally flushes instruction and data trace together whenever either flush request is seen but does not guarantee that the trace data has drained from the ETM. When the processor enters a low-power state, all trace data is output from the ETM.

### 15.4.8 Low-power state behavior

When the Cortex®-R82AE processor enters a low-power state, there is a delay before the resources in the ETM become inactive.

This permits the last instruction executed to trigger a comparator, update the counter or sequencer, and the resultant event packet to be inserted in the specified trace stream. This event packet is presented on the trace bus before the ETM itself enters a low-power state.

If an event packet is generated for a different reason, it is not guaranteed to be output before the ETM enters a low-power state, but is traced when the processor leaves the low-power state, if the ETM logic is not reset before this can occur.



The TRCEVENTCTL1R.LPOVERRIDE bit controls how a trace unit behaves in a low-power state. If it is set to 1, trace unit low-power state behavior is overridden, that is, entry to a low-power state does not affect the trace unit resources or trace generation. In this case, the ETM resources remain active.

### 15.4.9 Cycle counter

The Cortex®-R82AE processor ETM uses a 12-bit cycle counter.

The ETM cycle counter does not count when the Cortex®-R82AE processor is in a low-power state.

### 15.4.10 Non-architectural exceptions

Non-architectural behavior exceptions are indicated by the ETM.

The ETM indicates exceptions for the following non-architectural behavior that use the following TYPE encoding:

<b>0b10001</b>	ECC logic requires instruction trace to be replayed. This should not be relied on as providing trace of ECC behavior.
----------------	---

### 15.4.11 Trace synchronization

The ETM receives and combines all sources of trace synchronization requests to determine when synchronization is required. When synchronization is required, information is inserted in both trace streams as necessary (depending on whether data trace is active).

To decompress the trace streams, synchronization information in the data trace stream determines the alignment with synchronization information in the instruction stream. If the ETM is configured to trace only events in the data stream, you must configure the instruction trace stream to contain sufficient elements to permit the required data trace stream synchronization.

## 15.5 Modes of operation and execution

This section describes how to control the ETM programming and read and program the ETM registers.

### 15.5.1 Use of the ETM main enable bit

When programming the ETM registers, you must enable all the changes at the same time.

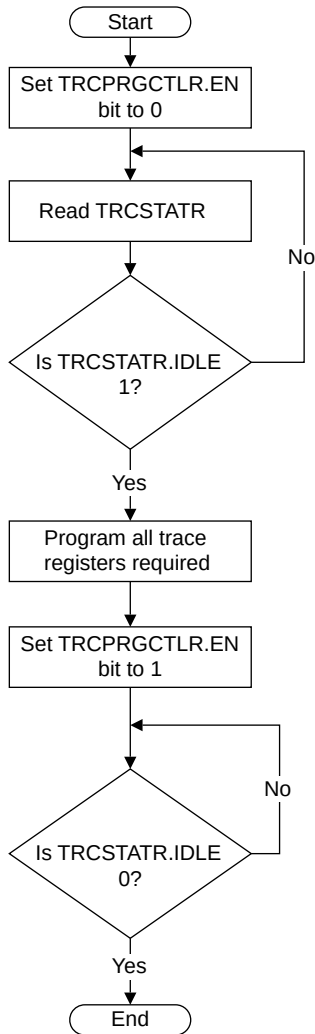
For example, if the counter is reprogrammed, it might start to count based on incorrect events, before the trigger condition has been correctly set up.

To disable all trace operations during programming use:

- The ETM main enable in the TRCPRGCTLR.
- The TRCSTATR to indicate the ETM status.

The Cortex®-R82AE processor does not have to be in Debug state while you program the ETM registers.

The following figure shows the procedure to use.

**Figure 15-3: Programming ETM registers**

### 15.5.2 Programming and reading ETM registers

To access the ETM registers, use the system register access. This provides a direct method of programming the ETM.

### 15.5.3 External register access permissions

Whether access is permitted to a register depends on:

- If the processor is powered up.
- The state of the OS Lock.

- The state of the debug authentication inputs to the processor.

The behavior that is specific to each register and the type of access to the register is not described in this document. For a detailed description of these features and their effects on the registers, see the [Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture](#).

The register descriptions provided in this section describe whether each register is read/write or read-only.

## 15.6 ETM register summary

The register summary tables provide an overview of all the relevant registers.

You can find the register summary table for the Cortex®-R82AE processor AArch64 *Embedded Trace Macrocell* (ETM) registers in [A.1.8 AArch64 Trace unit registers summary](#) on page 326.

You can find the register summary table for the core external ETM registers in [B.2.1.7 External ETM registers summary](#) on page 1717.

# 16. Advanced SIMD and floating-point support

This chapter introduces the optional Advanced SIMD and floating-point support.

## 16.1 About the Advanced SIMD and floating-point support

The Cortex®-R82AE processor supports the Advanced SIMD and scalar floating-point instructions in the Arm®v8-R AArch64 instruction set without floating-point exception trapping. The Cortex®-R82AE processor floating-point implementation includes several features from Armv8.2 and Arm®v8.3.

For more information on the architectural features that are implemented by the Cortex®-R82AE processor see, [3.2.1 Architecture requirements](#) on page 53.

Each core within the Cortex®-R82AE processor has optional Advanced SIMD and floating-point support.

The Cortex®-R82AE processor implements all scalar and vector operations in hardware with support for all combinations of:

- Rounding modes.
- Flush to-zero.
- Default Not a Number (NaN) modes.

The Arm®v8-R AArch64 architecture does not define a separate version number for its Advanced SIMD and floating-point support because the instructions are always implicitly present.

## 16.2 Low-latency single-precision instructions

The Cortex®-R82AE processor has a per-core `LOW_LATENCY_SP` parameter that controls the inclusion of additional hardware that exclusively processes scalar single-precision instructions.

If the `LOW_LATENCY_SP` is set to 0, the Advanced SIMD and scalar floating-point instructions complete in five cycles. If the `LOW_LATENCY_SP` is set to 1, an additional hardware is included that enables the scalar single-precision instructions to complete in three cycles.



Division and square root instructions take longer to complete. Scalar single-precision divisions and square roots are not sped up when `LOW_LATENCY_SP` is set to 1.

Including this feature enables your program to execute faster if and when using single-precision instructions.

The following table shows the scalar single-precision instructions that execute in three cycles when the `LOW_LATENCY_SP` = 1.

**Table 16-1: Low-latency scalar single-precision instructions**

Instruction	Conditions
FABD	sz == 0b0
FADD	ftype == 0b00
FMADD	ftype == 0b00
FMSUB	ftype == 0b00
FMUL	ftype == 0b00
FMULX	sz == 0b0
FMADD	ftype == 0b00
FNMSUB	ftype == 0b00
FMUL	ftype == 0b00
FRECPE	sz == 0b0
FRECPS	sz == 0b0
FRECPX	sz == 0b0
FRINTA/FRINTM/FRINTP/FRINTI/FRINTX/FRINTZ	ftype == 0b00
FRSQRT	sz == 0b0
FRSQRTS	sz == 0b0
FSUB	ftype == 0b00
SCVTF/UCVTF	ftype == 0b00

# Appendix A AArch64 registers

This appendix contains the descriptions for all the AArch64 registers in the Cortex®-R82AE processor.

## A.1 AArch64 register summaries

This section includes the register summary tables for all the AArch64 registers in the Cortex®-R82AE processor.

### A.1.1 AArch64 Identification registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Identification registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-1: Identification registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">MIDR_EL1</a>	3	0	C0	C0	0	See individual bit resets.	64-bit	Main ID Register
<a href="#">MPIDR_EL1</a>	3	0	C0	C0	5	See individual bit resets.	64-bit	Multiprocessor Affinity Register
<a href="#">REVIDR_EL1</a>	3	0	C0	C0	6	See individual bit resets.	64-bit	Revision ID Register
<a href="#">ID_PFR0_EL1</a>	3	0	C0	C1	0	See individual bit resets.	64-bit	AArch32 Processor Feature Register 0
<a href="#">ID_PFR1_EL1</a>	3	0	C0	C1	1	See individual bit resets.	64-bit	AArch32 Processor Feature Register 1
<a href="#">ID_DFR0_EL1</a>	3	0	C0	C1	2	See individual bit resets.	64-bit	AArch32 Debug Feature Register 0
<a href="#">ID_AFR0_EL1</a>	3	0	C0	C1	3	See individual bit resets.	64-bit	AArch32 Auxiliary Feature Register 0
<a href="#">ID_MMFR0_EL1</a>	3	0	C0	C1	4	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 0
<a href="#">ID_MMFR1_EL1</a>	3	0	C0	C1	5	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 1
<a href="#">ID_MMFR2_EL1</a>	3	0	C0	C1	6	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 2
<a href="#">ID_MMFR3_EL1</a>	3	0	C0	C1	7	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 3
<a href="#">ID_ISAR0_EL1</a>	3	0	C0	C2	0	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 0
<a href="#">ID_ISAR1_EL1</a>	3	0	C0	C2	1	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 1
<a href="#">ID_ISAR2_EL1</a>	3	0	C0	C2	2	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 2
<a href="#">ID_ISAR3_EL1</a>	3	0	C0	C2	3	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 3
<a href="#">ID_ISAR4_EL1</a>	3	0	C0	C2	4	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 4
<a href="#">ID_ISAR5_EL1</a>	3	0	C0	C2	5	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 5
<a href="#">ID_MMFR4_EL1</a>	3	0	C0	C2	6	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 4

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
ID_ISAR6_EL1	3	0	C0	C2	7	See individual bit resets.	64-bit	AArch32 Instruction Set Attribute Register 6
MVFR0_EL1	3	0	C0	C3	0	See individual bit resets.	64-bit	AArch32 Media and VFP Feature Register 0
MVFR1_EL1	3	0	C0	C3	1	See individual bit resets.	64-bit	AArch32 Media and VFP Feature Register 1
MVFR2_EL1	3	0	C0	C3	2	See individual bit resets.	64-bit	AArch32 Media and VFP Feature Register 2
ID_PFR2_EL1	3	0	C0	C3	4	See individual bit resets.	64-bit	AArch32 Processor Feature Register 2
ID_DFR1_EL1	3	0	C0	C3	5	See individual bit resets.	64-bit	Debug Feature Register 1
ID_MMFR5_EL1	3	0	C0	C3	6	See individual bit resets.	64-bit	AArch32 Memory Model Feature Register 5
ID_AA64PFR0_EL1	3	0	C0	C4	0	See individual bit resets.	64-bit	AArch64 Processor Feature Register 0
ID_AA64PFR1_EL1	3	0	C0	C4	1	See individual bit resets.	64-bit	AArch64 Processor Feature Register 1
ID_AA64DFR0_EL1	3	0	C0	C5	0	See individual bit resets.	64-bit	AArch64 Debug Feature Register 0
ID_AA64DFR1_EL1	3	0	C0	C5	1	See individual bit resets.	64-bit	AArch64 Debug Feature Register 1
ID_AA64AFR0_EL1	3	0	C0	C5	4	See individual bit resets.	64-bit	AArch64 Auxiliary Feature Register 0
ID_AA64AFR1_EL1	3	0	C0	C5	5	See individual bit resets.	64-bit	AArch64 Auxiliary Feature Register 1
ID_AA64ISAR0_EL1	3	0	C0	C6	0	See individual bit resets.	64-bit	AArch64 Instruction Set Attribute Register 0
ID_AA64ISAR1_EL1	3	0	C0	C6	1	See individual bit resets.	64-bit	AArch64 Instruction Set Attribute Register 1
ID_AA64ISAR2_EL1	3	0	C0	C6	2	See individual bit resets.	64-bit	AArch64 Instruction Set Attribute Register 2
ID_AA64MMFR0_EL1	3	0	C0	C7	0	See individual bit resets.	64-bit	AArch64 Memory Model Feature Register 0
ID_AA64MMFR1_EL1	3	0	C0	C7	1	See individual bit resets.	64-bit	AArch64 Memory Model Feature Register 1
ID_AA64MMFR2_EL1	3	0	C0	C7	2	See individual bit resets.	64-bit	AArch64 Memory Model Feature Register 2
ID_AA64MMFR3_EL1	3	0	C0	C7	3	See individual bit resets.	64-bit	AArch64 Memory Model Feature Register 3
CCSIDR_EL1	3	1	C0	C0	0	See individual bit resets.	64-bit	Current Cache Size ID Register
CLIDR_EL1	3	1	C0	C0	1	See individual bit resets.	64-bit	Cache Level ID Register
CSSELR_EL1	3	2	C0	C0	0	See individual bit resets.	64-bit	Cache Size Selection Register
CTR_EL0	3	3	C0	C0	1	See individual bit resets.	64-bit	Cache Type Register
DCZID_EL0	3	3	C0	C0	7	See individual bit resets.	64-bit	Data Cache Zero ID Register
VPIDR_EL2	3	4	C0	C0	0	See individual bit resets.	64-bit	Virtualization Processor ID Register
VMPIDR_EL2	3	4	C0	C0	5	See individual bit resets.	64-bit	Virtualization Multiprocessor ID Register

## A.1.2 AArch64 Generic System Control registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Generic System Control registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).



**Table A-2: Generic System Control registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
MPUIR_EL1	3	0	C0	C0	4	See individual bit resets.	64-bit	MPU Type Register (EL1)
SCTLR_EL1	3	0	C1	C0	0	See individual bit resets.	64-bit	System Control Register (EL1)
ACTLR_EL1	3	0	C1	C0	1	See individual bit resets.	64-bit	Auxiliary Control Register (EL1)
CPACR_EL1	3	0	C1	C0	2	See individual bit resets.	64-bit	Architectural Feature Access Control Register
TTBR0_EL1	3	0	C2	C0	0	See individual bit resets.	64-bit	Translation Table Base Register 0 (EL1)
TTBR1_EL1	3	0	C2	C0	1	See individual bit resets.	64-bit	Translation Table Base Register 1 (EL1)
TCR_EL1	3	0	C2	C0	2	See individual bit resets.	64-bit	Translation Control Register (EL1)
APIAKeyLo_EL1	3	0	C2	C1	0	See individual bit resets.	64-bit	Pointer Authentication Key A for Instruction (bits[63:0])
APIAKeyHi_EL1	3	0	C2	C1	1	See individual bit resets.	64-bit	Pointer Authentication Key A for Instruction (bits[127:64])
APIBKeyLo_EL1	3	0	C2	C1	2	See individual bit resets.	64-bit	Pointer Authentication Key B for Instruction (bits[63:0])
APIBKeyHi_EL1	3	0	C2	C1	3	See individual bit resets.	64-bit	Pointer Authentication Key B for Instruction (bits[127:64])
APDAKeyLo_EL1	3	0	C2	C2	0	See individual bit resets.	64-bit	Pointer Authentication Key A for Data (bits[63:0])
APDAKeyHi_EL1	3	0	C2	C2	1	See individual bit resets.	64-bit	Pointer Authentication Key A for Data (bits[127:64])
APDBKeyLo_EL1	3	0	C2	C2	2	See individual bit resets.	64-bit	Pointer Authentication Key B for Data (bits[63:0])
APDBKeyHi_EL1	3	0	C2	C2	3	See individual bit resets.	64-bit	Pointer Authentication Key B for Data (bits[127:64])
APGAKeyLo_EL1	3	0	C2	C3	0	See individual bit resets.	64-bit	Pointer Authentication Key A for Code (bits[63:0])
APGAKeyHi_EL1	3	0	C2	C3	1	See individual bit resets.	64-bit	Pointer Authentication Key A for Code (bits[127:64])
SPSel	3	0	C4	C2	0	See individual bit resets.	64-bit	Stack Pointer Select
CurrentEL	3	0	C4	C2	2	See individual bit resets.	64-bit	Current Exception Level
PAN	3	0	C4	C2	3	See individual bit resets.	64-bit	Privileged Access Never
UAO	3	0	C4	C2	4	See individual bit resets.	64-bit	User Access Override
AFSR0_EL1	3	0	C5	C1	0	See individual bit resets.	64-bit	Auxiliary Fault Status Register 0 (EL1)
AFSR1_EL1	3	0	C5	C1	1	See individual bit resets.	64-bit	Auxiliary Fault Status Register 1 (EL1)

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
ESR_EL1	3	0	C5	C2	0	See individual bit resets.	64-bit	Exception Syndrome Register (EL1)
PRBAR<n>_EL1	3	0	C6	1:m[3:1]	m[0]:00	See individual bit resets.	64-bit	Protection Region Base Address Register n (EL1)
PRLAR<n>_EL1	3	0	C6	1:m[3:1]	m[0]:01	See individual bit resets.	64-bit	Protection Region Limit Address Register n (EL1)
FAR_EL1	3	0	C6	C0	0	See individual bit resets.	64-bit	Fault Address Register (EL1)
PRENR_EL1	3	0	C6	C1	1	See individual bit resets.	64-bit	Protection Region Enable Register (EL1)
PRSELR_EL1	3	0	C6	C2	1	See individual bit resets.	64-bit	Protection Region Selection Register (EL1)
PRBAR_EL1	3	0	C6	C8	0	See individual bit resets.	64-bit	Protection Region Base Address Register (EL1)
PRLAR_EL1	3	0	C6	C8	1	See individual bit resets.	64-bit	Protection Region Limit Address Register (EL1)
PAR_EL1	3	0	C7	C4	0	See individual bit resets.	64-bit	Physical Address Register
MAIR_EL1	3	0	C10	C2	0	See individual bit resets.	64-bit	Memory Attribute Indirection Register (EL1)
AMAIR_EL1	3	0	C10	C3	0	See individual bit resets.	64-bit	Auxiliary Memory Attribute Indirection Register (EL1)
VBAR_EL1	3	0	C12	C0	0	See individual bit resets.	64-bit	Vector Base Address Register (EL1)
ISR_EL1	3	0	C12	C1	0	See individual bit resets.	64-bit	Interrupt Status Register
CONTEXTIDR_EL1	3	0	C13	C0	1	See individual bit resets.	64-bit	Context ID Register (EL1)
TPIDR_EL1	3	0	C13	C0	4	See individual bit resets.	64-bit	EL1 Software Thread ID Register
IMP_ITCMREGIONR_EL1	3	0	C15	C0	1	See individual bit resets.	64-bit	ITCM Region Register
IMP_DTCMREGIONR_EL1	3	0	C15	C0	2	See individual bit resets.	64-bit	DTCM Region Register
IMP_LLPPREGIONR_EL1	3	0	C15	C0	3	See individual bit resets.	64-bit	LLPP Region Register
IMP_LLRAMREGIONR_EL1	3	0	C15	C0	4	See individual bit resets.	64-bit	LLRAM Region Register
IMP_SPPREGIONR_EL1	3	0	C15	C0	5	See individual bit resets.	64-bit	SPP Region Register
IMP_CPUACTLR_EL1	3	0	C15	C1	0	See individual bit resets.	64-bit	CPU Auxiliary Control Register
IMP_BPCTLR_EL1	3	0	C15	C1	1	See individual bit resets.	64-bit	Branch Predictor Control Register
IMP_CPUBUSTIMEOUTR_EL1	3	0	C15	C1	2	See individual bit resets.	64-bit	CPU Bus Timeout Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
IMP_INTMONR_EL1	3	0	C15	C1	3	See individual bit resets.	64-bit	Interrupt Monitoring Register
IMP_MEMPROTCTLR_EL1	3	0	C15	C1	5	See individual bit resets.	64-bit	Memory Protection Control Register
IMP_CPUCFR_EL1	3	0	C15	C2	0	See individual bit resets.	64-bit	CPU Configuration Register
IMP_CPUPWRCTLR_EL1	3	0	C15	C2	7	See individual bit resets.	64-bit	CPU Power Control Register
IMP_CLUSTERCFR_EL1	3	0	C15	C3	0	See individual bit resets.	64-bit	Cluster Configuration Register
IMP_CLUSTERBUSTIMEOUTR_EL1	3	0	C15	C3	2	See individual bit resets.	64-bit	Cluster Bus Timeout Register
IMP_CLUSTERACTLR_EL1	3	0	C15	C3	3	See individual bit resets.	64-bit	Cluster Auxiliary Control Register
IMP_CLUSTERPWRCTLR_EL1	3	0	C15	C3	5	See individual bit resets.	64-bit	Cluster Power Control Register
IMP_CLUSTERPWRDN_EL1	3	0	C15	C3	6	See individual bit resets.	64-bit	Cluster Power Down Register
IMP_CLUSTERPWRSTAT_EL1	3	0	C15	C3	7	See individual bit resets.	64-bit	Cluster Power Status Register
IMP_CLUSTERSID_EL1	3	0	C15	C4	0	See individual bit resets.	64-bit	Cluster Scheme ID Register
IMP_CLUSTERACPSID_EL1	3	0	C15	C4	1	See individual bit resets.	64-bit	Cluster ACP Scheme ID Register
IMP_CLUSTERPARTCR_EL1	3	0	C15	C4	3	See individual bit resets.	64-bit	Cluster Partition Control Register
IMP_CLUSTERQOSR_EL1	3	0	C15	C4	4	See individual bit resets.	64-bit	Cluster Quality of Service Register
IMP_CLUSTERACELSCTLR_EL1	3	0	C15	C4	5	See individual bit resets.	64-bit	ACELS Port Control Register
IMP_CLUSTERMEMPROTCTLR_EL1	3	0	C15	C4	6	See individual bit resets.	64-bit	Cluster Memory Protection Control Register
AIDR_EL1	3	1	C0	C0	7	See individual bit resets.	64-bit	Auxiliary ID Register
IMP_CDBGDR0_EL1	3	2	C15	C0	0	See individual bit resets.	64-bit	Cache Debug Data Register 0
IMP_CDBGDR1_EL1	3	2	C15	C0	1	See individual bit resets.	64-bit	Cache Debug Data Register 1
IMP_CLUSTERCDBGDR0_EL1	3	2	C15	C3	0	See individual bit resets.	64-bit	Cluster Cache Debug Data Register 0
IMP_CPUPSELR_EL1	3	2	C15	C8	0	See individual bit resets.	64-bit	Instruction Patch Selection Register
IMP_CPUPCR_EL1	3	2	C15	C8	1	See individual bit resets.	64-bit	Selected Instruction Patch Control Register
IMP_CPUPCR<n>_EL1	3	2	C15	C8	1	See individual bit resets.	64-bit	Instruction Patch Control Registers

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
IMP_CPUPOR_EL1	3	2	C15	C8	2	See individual bit resets.	64-bit	Selected Instruction Patch Opcode Register
IMP_CPUPOR<n>_EL1	3	2	C15	C8	2	See individual bit resets.	64-bit	Instruction Patch Opcode Registers
IMP_CPUPMR_EL1	3	2	C15	C8	3	See individual bit resets.	64-bit	Selected Instruction Patch Mask Register
IMP_CPUPMR<n>_EL1	3	2	C15	C8	3	See individual bit resets.	64-bit	Instruction Patch Mask Registers
NZCV	3	3	C4	C2	0	See individual bit resets.	64-bit	Condition Flags
DAIF	3	3	C4	C2	1	See individual bit resets.	64-bit	Interrupt Mask Bits
DIT	3	3	C4	C2	5	See individual bit resets.	64-bit	Data Independent Timing
SSBS	3	3	C4	C2	6	See individual bit resets.	64-bit	Speculative Store Bypass Safe
FPCR	3	3	C4	C4	0	See individual bit resets.	64-bit	Floating-point Control Register
FPSR	3	3	C4	C4	1	See individual bit resets.	64-bit	Floating-point Status Register
TPIDR_ELO	3	3	C13	C0	2	See individual bit resets.	64-bit	ELO Read/Write Software Thread ID Register
TPIDRRO_ELO	3	3	C13	C0	3	See individual bit resets.	64-bit	ELO Read-Only Software Thread ID Register
MPUIR_EL2	3	4	C0	C0	4	See individual bit resets.	64-bit	MPU Type Register (EL2)
ACTLR_EL2	3	4	C1	C0	1	See individual bit resets.	64-bit	Auxiliary Control Register (EL2)
HCR_EL2	3	4	C1	C1	0	See individual bit resets.	64-bit	Hypervisor Configuration Register
CPTR_EL2	3	4	C1	C1	2	See individual bit resets.	64-bit	Architectural Feature Trap Register (EL2)
HACR_EL2	3	4	C1	C1	7	See individual bit resets.	64-bit	Hypervisor Auxiliary Control Register
VSCTLR_EL2	3	4	C2	C0	0	See individual bit resets.	64-bit	Virtualization System Control Register (EL2)
TCR_EL2	3	4	C2	C0	2	See individual bit resets.	64-bit	Translation Control Register (EL2)
VTCR_EL2	3	4	C2	C1	2	See individual bit resets.	64-bit	Virtualization Translation Control Register
VSTCR_EL2	3	4	C2	C6	2	See individual bit resets.	64-bit	Virtualization Secure Translation Control Register
AFSR0_EL2	3	4	C5	C1	0	See individual bit resets.	64-bit	Auxiliary Fault Status Register 0 (EL2)
AFSR1_EL2	3	4	C5	C1	1	See individual bit resets.	64-bit	Auxiliary Fault Status Register 1 (EL2)

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
ESR_EL2	3	4	C5	C2	0	See individual bit resets.	64-bit	Exception Syndrome Register (EL2)
PRBAR<n>_EL2	3	4	C6	1:m[3:1]	m[0]:00	See individual bit resets.	64-bit	Protection Region Base Address Register n (EL2)
PRLAR<n>_EL2	3	4	C6	1:m[3:1]	m[0]:01	See individual bit resets.	64-bit	Protection Region Limit Address Register n (EL2)
FAR_EL2	3	4	C6	C0	0	See individual bit resets.	64-bit	Fault Address Register (EL2)
HPFAR_EL2	3	4	C6	C0	4	See individual bit resets.	64-bit	Hypervisor IPA Fault Address Register
PRENR_EL2	3	4	C6	C1	1	See individual bit resets.	64-bit	Protection Region Enable Register (EL2)
PRSELR_EL2	3	4	C6	C2	1	See individual bit resets.	64-bit	Protection Region Selection Register (EL2)
PRBAR_EL2	3	4	C6	C8	0	See individual bit resets.	64-bit	Protection Region Base Address Register (EL2)
PRLAR_EL2	3	4	C6	C8	1	See individual bit resets.	64-bit	Protection Region Limit Address Register (EL2)
MAIR_EL2	3	4	C10	C2	0	See individual bit resets.	64-bit	Memory Attribute Indirection Register (EL2)
AMAIR_EL2	3	4	C10	C3	0	See individual bit resets.	64-bit	Auxiliary Memory Attribute Indirection Register (EL2)
VBAR_EL2	3	4	C12	C0	0	See individual bit resets.	64-bit	Vector Base Address Register (EL2)
RVBAR_EL2	3	4	C12	C0	1	See individual bit resets.	64-bit	Reset Vector Base Address Register (if EL3 not implemented)
RMR_EL2	3	4	C12	C0	2	See individual bit resets.	64-bit	Reset Management Register (EL2)
CONTEXTIDR_EL2	3	4	C13	C0	1	See individual bit resets.	64-bit	Context ID Register (EL2)
TPIDR_EL2	3	4	C13	C0	2	See individual bit resets.	64-bit	EL2 Software Thread ID Register
IMP_INTLATENCY_EL2	3	4	C15	C1	7	See individual bit resets.	64-bit	Interrupt Latency Register

### A.1.3 AArch64 Performance Monitors registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Performance Monitors registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-3: Performance Monitors registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
PMINTENSET_EL1	3	0	C9	C14	1	See individual bit resets.	64-bit	Performance Monitors Interrupt Enable Set Register
PMINTENCLR_EL1	3	0	C9	C14	2	See individual bit resets.	64-bit	Performance Monitors Interrupt Enable Clear Register
PMMIR_EL1	3	0	C9	C14	6	See individual bit resets.	64-bit	Performance Monitors Machine Identification Register
IMP_CLUSTERPMCR_EL1	3	0	C15	C5	0	See individual bit resets.	64-bit	Cluster Performance Monitors Control Register
IMP_CLUSTERPMCNTENSET_EL1	3	0	C15	C5	1	See individual bit resets.	64-bit	Cluster Performance Monitors Count Enable Set register
IMP_CLUSTERPMCNTENCLR_EL1	3	0	C15	C5	2	See individual bit resets.	64-bit	Cluster Performance Monitors Count Enable Clear register
IMP_CLUSTERPMOVSSSET_EL1	3	0	C15	C5	3	See individual bit resets.	64-bit	Cluster Performance Monitors Overflow Flag Status Set register
IMP_CLUSTERPMOVSLCLR_EL1	3	0	C15	C5	4	See individual bit resets.	64-bit	Cluster Performance Monitors Overflow Flag Status Clear Register
IMP_CLUSTERPMSELR_EL1	3	0	C15	C5	5	See individual bit resets.	64-bit	Cluster Performance Monitors Event Counter Selection Register
IMP_CLUSTERPMINTENSET_EL1	3	0	C15	C5	6	See individual bit resets.	64-bit	Cluster Performance Monitors Interrupt Enable Set register
IMP_CLUSTERPMINTENCLR_EL1	3	0	C15	C5	7	See individual bit resets.	64-bit	Cluster Performance Monitors Interrupt Enable Clear register
IMP_CLUSTERPMCCNTR_EL1	3	0	C15	C6	0	See individual bit resets.	64-bit	Cluster Performance Monitors Cycle Count Register
IMP_CLUSTERPMXEVTYPER_EL1	3	0	C15	C6	1	See individual bit resets.	64-bit	Cluster Performance Monitors Selected Event Type Register
IMP_CLUSTERPMXEVCNTR_EL1	3	0	C15	C6	2	See individual bit resets.	64-bit	Cluster Performance Monitors Selected Event Count Register
IMP_CLUSTERPMCEID0_EL1	3	0	C15	C6	4	See individual bit resets.	64-bit	Cluster Performance Monitors Common Event Identification register 0
IMP_CLUSTERPMCEID1_EL1	3	0	C15	C6	5	See individual bit resets.	64-bit	Cluster Performance Monitors Common Event Identification register 1
IMP_CLUSTERPMCLAIMSET_EL1	3	0	C15	C6	6	See individual bit resets.	64-bit	Cluster Performance Monitors Claim Set register
IMP_CLUSTERPMCLAIMCLR_EL1	3	0	C15	C6	7	See individual bit resets.	64-bit	Cluster Performance Monitors Claim Clear register
PMCR_ELO	3	3	C9	C12	0	See individual bit resets.	64-bit	Performance Monitors Control Register
PMCNTENSET_ELO	3	3	C9	C12	1	See individual bit resets.	64-bit	Performance Monitors Count Enable Set Register
PMCNTENCLR_ELO	3	3	C9	C12	2	See individual bit resets.	64-bit	Performance Monitors Count Enable Clear Register
PMOVSLCLR_ELO	3	3	C9	C12	3	See individual bit resets.	64-bit	Performance Monitors Overflow Flag Status Clear Register
PMSWINC_ELO	3	3	C9	C12	4	See individual bit resets.	64-bit	Performance Monitors Software Increment Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
PMSELR_ELO	3	3	C9	C12	5	See individual bit resets.	64-bit	Performance Monitors Event Counter Selection Register
PMCEID0_ELO	3	3	C9	C12	6	See individual bit resets.	64-bit	Performance Monitors Common Event Identification Register 0
PMCEID1_ELO	3	3	C9	C12	7	See individual bit resets.	64-bit	Performance Monitors Common Event Identification Register 1
PMCCNTR_ELO	3	3	C9	C13	0	See individual bit resets.	64-bit	Performance Monitors Cycle Count Register
PMXEVTYPER_ELO	3	3	C9	C13	1	See individual bit resets.	64-bit	Performance Monitors Selected Event Type Register
PMXVCNTR_ELO	3	3	C9	C13	2	See individual bit resets.	64-bit	Performance Monitors Selected Event Count Register
PMUSERENR_ELO	3	3	C9	C14	0	See individual bit resets.	64-bit	Performance Monitors User Enable Register
PMOVSSET_ELO	3	3	C9	C14	3	See individual bit resets.	64-bit	Performance Monitors Overflow Flag Status Set Register
PMEVCNTR<n>_ELO	3	3	C14	10:m[4:3]	m[2:0]	See individual bit resets.	64-bit	Performance Monitors Event Count Registers
PMEVTYPER<n>_ELO	3	3	C14	11:m[4:3]	m[2:0]	See individual bit resets.	64-bit	Performance Monitors Event Type Registers
PMCCFILTR_ELO	3	3	C14	C15	7	See individual bit resets.	64-bit	Performance Monitors Cycle Count Filter Register

## A.1.4 AArch64 System instructions summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** System instructions in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-4: System instructions summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
IC_IALLUIS	1	0	C7	C1	0	See individual bit resets.	64-bit	Instruction Cache Invalidate All to PoU, Inner Shareable
IC_IALLU	1	0	C7	C5	0	See individual bit resets.	64-bit	Instruction Cache Invalidate All to PoU
DC_IVAC	1	0	C7	C6	1	See individual bit resets.	64-bit	Data or unified Cache line Invalidate by VA to PoC

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
DC_ISW	1	0	C7	C6	2	See individual bit resets.	64-bit	Data or unified Cache line Invalidate by Set/Way
AT_S1E1R	1	0	C7	C8	0	See individual bit resets.	64-bit	Address Translate Stage 1 EL1 Read
AT_S1E1W	1	0	C7	C8	1	See individual bit resets.	64-bit	Address Translate Stage 1 EL1 Write
AT_S1E0R	1	0	C7	C8	2	See individual bit resets.	64-bit	Address Translate Stage 1 ELO Read
AT_S1E0W	1	0	C7	C8	3	See individual bit resets.	64-bit	Address Translate Stage 1 ELO Write
AT_S1E1RP	1	0	C7	C9	0	See individual bit resets.	64-bit	Address Translate Stage 1 EL1 Read PAN
AT_S1E1WP	1	0	C7	C9	1	See individual bit resets.	64-bit	Address Translate Stage 1 EL1 Write PAN
DC_CSW	1	0	C7	C10	2	See individual bit resets.	64-bit	Data or unified Cache line Clean by Set/Way
DC_CISW	1	0	C7	C14	2	See individual bit resets.	64-bit	Data or unified Cache line Clean and Invalidate by Set/Way
TLBI_VMALE1OS	1	0	C8	C1	0	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at stage 1, EL1, Outer Shareable
TLBI_VAE1OS	1	0	C8	C1	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL1, Outer Shareable
TLBI_ASIDE1OS	1	0	C8	C1	2	See individual bit resets.	64-bit	TLB Invalidate by ASID, EL1, Outer Shareable
TLBI_VAAE1OS	1	0	C8	C1	3	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, EL1, Outer Shareable
TLBI_VALE1OS	1	0	C8	C1	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL1, Outer Shareable
TLBI_VAALE1OS	1	0	C8	C1	7	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, Last Level, EL1, Outer Shareable
TLBI_RVAE1IS	1	0	C8	C2	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL1, Inner Shareable



Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TLBI_RVAAE1IS	1	0	C8	C2	3	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, EL1, Inner Shareable
TLBI_RVALE1IS	1	0	C8	C2	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL1, Inner Shareable
TLBI_RVAALE1IS	1	0	C8	C2	7	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, Last Level, EL1, Inner Shareable
TLBI_VMALE1IS	1	0	C8	C3	0	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at stage 1, EL1, Inner Shareable
TLBI_VAE1IS	1	0	C8	C3	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL1, Inner Shareable
TLBI_ASIDE1IS	1	0	C8	C3	2	See individual bit resets.	64-bit	TLB Invalidate by ASID, EL1, Inner Shareable
TLBI_VAAE1IS	1	0	C8	C3	3	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, EL1, Inner Shareable
TLBI_VALE1IS	1	0	C8	C3	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL1, Inner Shareable
TLBI_VAALE1IS	1	0	C8	C3	7	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, Last Level, EL1, Inner Shareable
TLBI_RVAE1OS	1	0	C8	C5	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL1, Outer Shareable
TLBI_RVAAE1OS	1	0	C8	C5	3	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, EL1, Outer Shareable
TLBI_RVALE1OS	1	0	C8	C5	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL1, Outer Shareable
TLBI_RVAALE1OS	1	0	C8	C5	7	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, Last Level, EL1, Outer Shareable
TLBI_RVAE1	1	0	C8	C6	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL1
TLBI_RVAAE1	1	0	C8	C6	3	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, EL1
TLBI_RVALE1	1	0	C8	C6	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL1

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TLBI_RVAAL1	1	0	C8	C6	7	See individual bit resets.	64-bit	TLB Range Invalidate by VA, All ASID, Last level, EL1
TLBI_VMAL1	1	0	C8	C7	0	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at stage 1, EL1
TLBI_VA1	1	0	C8	C7	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL1
TLBI_ASID1	1	0	C8	C7	2	See individual bit resets.	64-bit	TLB Invalidate by ASID, EL1
TLBI_VAA1	1	0	C8	C7	3	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, EL1
TLBI_VA1	1	0	C8	C7	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL1
TLBI_VAA1	1	0	C8	C7	7	See individual bit resets.	64-bit	TLB Invalidate by VA, All ASID, Last level, EL1
SYS_IMP_BPI	1	0	C15	C1	1	See individual bit resets.	64-bit	Branch Predictor Invalidation Operation
SYS_IMP_IQBAR	1	0	C15	C1	2	See individual bit resets.	64-bit	STL Instruction Queue Barrier Operation
SYS_IMP_DFBSTL	1	0	C15	C1	3	See individual bit resets.	64-bit	STL Data Full Barrier Operation
SYS_IMP_CDBGDCT	1	2	C15	C2	0	See individual bit resets.	64-bit	L1 Data Cache Tag Read Operation
SYS_IMP_CDBGICT	1	2	C15	C2	1	See individual bit resets.	64-bit	L1 Instruction Cache Tag Read Operation
SYS_IMP_CDBGTT	1	2	C15	C2	2	See individual bit resets.	64-bit	TLB Tag Read Operation
SYS_IMP_CLUSTERCDBGL2T	1	2	C15	C2	3	See individual bit resets.	64-bit	L2 Cache Tag Read Operation
SYS_IMP_CLUSTERCDBGL2DT	1	2	C15	C3	3	See individual bit resets.	64-bit	L2 Cache Duplicate L1 Tag Read Operation
SYS_IMP_CLUSTERCDBGLCUDT	1	2	C15	C3	4	See individual bit resets.	64-bit	LCU Duplicate L1 Tag Read Operation

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
SYS_IMP_CDBGDCD	1	2	C15	C4	0	See individual bit resets.	64-bit	L1 Data Cache Data Read Operation
SYS_IMP_CDBGICD	1	2	C15	C4	1	See individual bit resets.	64-bit	L1 Instruction Cache Data Read Operation
SYS_IMP_CDBGTD	1	2	C15	C4	2	See individual bit resets.	64-bit	TLB Data Read Operation
SYS_IMP_CLUSTERCDBGL2D	1	2	C15	C4	3	See individual bit resets.	64-bit	L2 Cache Data Read Operation
CFP_RCTX	1	3	C7	C3	4	See individual bit resets.	64-bit	Control Flow Prediction Restriction by Context
DVP_RCTX	1	3	C7	C3	5	See individual bit resets.	64-bit	Data Value Prediction Restriction by Context
CPP_RCTX	1	3	C7	C3	7	See individual bit resets.	64-bit	Cache Prefetch Prediction Restriction by Context
DC_ZVA	1	3	C7	C4	1	See individual bit resets.	64-bit	Data Cache Zero by VA
IC_IVAU	1	3	C7	C5	1	See individual bit resets.	64-bit	Instruction Cache line Invalidate by VA to PoU
DC_CVAC	1	3	C7	C10	1	See individual bit resets.	64-bit	Data or unified Cache line Clean by VA to PoC
DC_CVAU	1	3	C7	C11	1	See individual bit resets.	64-bit	Data or unified Cache line Clean by VA to PoU
DC_CVAP	1	3	C7	C12	1	See individual bit resets.	64-bit	Data or unified Cache line Clean by VA to PoP
DC_CVADP	1	3	C7	C13	1	See individual bit resets.	64-bit	Data or unified Cache line Clean by VA to PoDP
DC_CIVAC	1	3	C7	C14	1	See individual bit resets.	64-bit	Data or unified Cache line Clean and Invalidate by VA to PoC
AT_S1E2R	1	4	C7	C8	0	See individual bit resets.	64-bit	Address Translate Stage 1 EL2 Read
AT_S1E2W	1	4	C7	C8	1	See individual bit resets.	64-bit	Address Translate Stage 1 EL2 Write

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
AT_S12E1R	1	4	C7	C8	4	See individual bit resets.	64-bit	Address Translate Stages 1 and 2 EL1 Read
AT_S12E1W	1	4	C7	C8	5	See individual bit resets.	64-bit	Address Translate Stages 1 and 2 EL1 Write
AT_S12E0R	1	4	C7	C8	6	See individual bit resets.	64-bit	Address Translate Stages 1 and 2 EL0 Read
AT_S12E0W	1	4	C7	C8	7	See individual bit resets.	64-bit	Address Translate Stages 1 and 2 EL0 Write
TLBI_IPAS2E1IS	1	4	C8	C0	1	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, EL1, Inner Shareable
TLBI_RIPAS2E1IS	1	4	C8	C0	2	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1, Inner Shareable
TLBI_IPAS2LE1IS	1	4	C8	C0	5	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Inner Shareable
TLBI_RIPAS2LE1IS	1	4	C8	C0	6	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Inner Shareable
TLBI_ALLE2OS	1	4	C8	C1	0	See individual bit resets.	64-bit	TLB Invalidate All, EL2, Outer Shareable
TLBI_VAE2OS	1	4	C8	C1	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL2, Outer Shareable
TLBI_ALLE1OS	1	4	C8	C1	4	See individual bit resets.	64-bit	TLB Invalidate All, EL1, Outer Shareable
TLBI_VALE2OS	1	4	C8	C1	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL2, Outer Shareable
TLBI_VMALLS12E1OS	1	4	C8	C1	6	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at Stage 1 and 2, EL1, Outer Shareable
TLBI_RVAE2IS	1	4	C8	C2	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL2, Inner Shareable
TLBI_RVALE2IS	1	4	C8	C2	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL2, Inner Shareable
TLBI_ALLE2IS	1	4	C8	C3	0	See individual bit resets.	64-bit	TLB Invalidate All, EL2, Inner Shareable

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TLBI_VAE2IS	1	4	C8	C3	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL2, Inner Shareable
TLBI_ALLE1IS	1	4	C8	C3	4	See individual bit resets.	64-bit	TLB Invalidate All, EL1, Inner Shareable
TLBI_VALE2IS	1	4	C8	C3	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL2, Inner Shareable
TLBI_VMALLS12E1IS	1	4	C8	C3	6	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at Stage 1 and 2, EL1, Inner Shareable
TLBI_IPAS2E1OS	1	4	C8	C4	0	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, EL1, Outer Shareable
TLBI_IPAS2E1	1	4	C8	C4	1	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, EL1
TLBI_RIPAS2E1	1	4	C8	C4	2	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1
TLBI_RIPAS2E1OS	1	4	C8	C4	3	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1, Outer Shareable
TLBI_IPAS2LE1OS	1	4	C8	C4	4	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Outer Shareable
TLBI_IPAS2LE1	1	4	C8	C4	5	See individual bit resets.	64-bit	TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1
TLBI_RIPAS2LE1	1	4	C8	C4	6	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1
TLBI_RIPAS2LE1OS	1	4	C8	C4	7	See individual bit resets.	64-bit	TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Outer Shareable
TLBI_RVAE2OS	1	4	C8	C5	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL2, Outer Shareable
TLBI_RVALE2OS	1	4	C8	C5	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL2, Outer Shareable
TLBI_RVAE2	1	4	C8	C6	1	See individual bit resets.	64-bit	TLB Range Invalidate by VA, EL2
TLBI_RVALE2	1	4	C8	C6	5	See individual bit resets.	64-bit	TLB Range Invalidate by VA, Last level, EL2

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TLBI_ALLE2	1	4	C8	C7	0	See individual bit resets.	64-bit	TLB Invalidate All, EL2
TLBI_VAE2	1	4	C8	C7	1	See individual bit resets.	64-bit	TLB Invalidate by VA, EL2
TLBI_ALLE1	1	4	C8	C7	4	See individual bit resets.	64-bit	TLB Invalidate All, EL1
TLBI_VALE2	1	4	C8	C7	5	See individual bit resets.	64-bit	TLB Invalidate by VA, Last level, EL2
TLBI_VMALLS12E1	1	4	C8	C7	6	See individual bit resets.	64-bit	TLB Invalidate by VMID, All at Stage 1 and 2, EL1

### A.1.5 AArch64 Debug registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Debug registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-5: Debug registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
OSDTRRX_EL1	2	0	C0	C0	2	See individual bit resets.	64-bit	OS Lock Data Transfer Register, Receive
MDCCINT_EL1	2	0	C0	C2	0	See individual bit resets.	64-bit	Monitor DCC Interrupt Enable Register
MDSCR_EL1	2	0	C0	C2	2	See individual bit resets.	64-bit	Monitor Debug System Control Register
OSDTRTX_EL1	2	0	C0	C3	2	See individual bit resets.	64-bit	OS Lock Data Transfer Register, Transmit
OSECCR_EL1	2	0	C0	C6	2	See individual bit resets.	64-bit	OS Lock Exception Catch Control Register
DBGBVR<n>_EL1	2	0	C0	m[3:0]	4	See individual bit resets.	64-bit	Debug Breakpoint Value Registers
DBGBCR<n>_EL1	2	0	C0	m[3:0]	5	See individual bit resets.	64-bit	Debug Breakpoint Control Registers
DBGWVR<n>_EL1	2	0	C0	m[3:0]	6	See individual bit resets.	64-bit	Debug Watchpoint Value Registers
DBGWCR<n>_EL1	2	0	C0	m[3:0]	7	See individual bit resets.	64-bit	Debug Watchpoint Control Registers
MDRAR_EL1	2	0	C1	C0	0	See individual bit resets.	64-bit	Monitor Debug ROM Address Register
OSLAR_EL1	2	0	C1	C0	4	See individual bit resets.	64-bit	OS Lock Access Register
OSLSR_EL1	2	0	C1	C1	4	See individual bit resets.	64-bit	OS Lock Status Register
OSDLR_EL1	2	0	C1	C3	4	See individual bit resets.	64-bit	OS Double Lock Register
DBGPRCR_EL1	2	0	C1	C4	4	See individual bit resets.	64-bit	Debug Power Control Register
DBGCLAIMSET_EL1	2	0	C7	C8	6	See individual bit resets.	64-bit	Debug CLAIM Tag Set Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
DBGCLAIMCLR_EL1	2	0	C7	C9	6	See individual bit resets.	64-bit	Debug CLAIM Tag Clear Register
DBGAUTHSTATUS_EL1	2	0	C7	C14	6	See individual bit resets.	64-bit	Debug Authentication Status Register
MDCCSR_ELO	2	3	C0	C1	0	See individual bit resets.	64-bit	Monitor DCC Status Register
DBGDTR_ELO	2	3	C0	C4	0	See individual bit resets.	64-bit	Debug Data Transfer Register, half-duplex
DBGDTRRX_ELO	2	3	C0	C5	0	See individual bit resets.	64-bit	Debug Data Transfer Register, Receive
DBGDTRTX_ELO	2	3	C0	C5	0	See individual bit resets.	64-bit	Debug Data Transfer Register, Transmit
TRFCR_EL1	3	0	C1	C2	1	See individual bit resets.	64-bit	Trace Filter Control Register (EL1)
MDCR_EL2	3	4	C1	C1	1	See individual bit resets.	64-bit	Monitor Debug Configuration Register (EL2)
TRFCR_EL2	3	4	C1	C2	1	See individual bit resets.	64-bit	Trace Filter Control Register (EL2)

## A.1.6 AArch64 GIC system registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** GIC system registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-6: GIC system registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
ICC_PMR_EL1	3	0	C4	C6	0	See individual bit resets.	64-bit	Interrupt Controller Interrupt Priority Mask Register
ICV_PMR_EL1	3	0	C4	C6	0	See individual bit resets.	64-bit	Interrupt Controller Virtual Interrupt Priority Mask Register
ICC_IAR0_EL1	3	0	C12	C8	0	See individual bit resets.	64-bit	Interrupt Controller Interrupt Acknowledge Register 0
ICV_IAR0_EL1	3	0	C12	C8	0	See individual bit resets.	64-bit	Interrupt Controller Virtual Interrupt Acknowledge Register 0
ICC_EOIRO_EL1	3	0	C12	C8	1	See individual bit resets.	64-bit	Interrupt Controller End Of Interrupt Register 0
ICV_EOIRO_EL1	3	0	C12	C8	1	See individual bit resets.	64-bit	Interrupt Controller Virtual End Of Interrupt Register 0
ICC_AP0R<n>_EL1	3	0	C12	C8	1:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Active Priorities Group 0 Registers
ICV_AP0R<n>_EL1	3	0	C12	C8	1:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Virtual Active Priorities Group 0 Registers
ICC_HPPIRO_EL1	3	0	C12	C8	2	See individual bit resets.	64-bit	Interrupt Controller Highest Priority Pending Interrupt Register 0
ICV_HPPIRO_EL1	3	0	C12	C8	2	See individual bit resets.	64-bit	Interrupt Controller Virtual Highest Priority Pending Interrupt Register 0

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
ICV_BPR0_EL1	3	0	C12	C8	3	See individual bit resets.	64-bit	Interrupt Controller Virtual Binary Point Register 0
ICC_AP1R<n>_EL1	3	0	C12	C9	0:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Active Priorities Group 1 Registers
ICV_AP1R<n>_EL1	3	0	C12	C9	0:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Virtual Active Priorities Group 1 Registers
ICC_DIR_EL1	3	0	C12	C11	1	See individual bit resets.	64-bit	Interrupt Controller Deactivate Interrupt Register
ICV_DIR_EL1	3	0	C12	C11	1	See individual bit resets.	64-bit	Interrupt Controller Deactivate Virtual Interrupt Register
ICC_RPR_EL1	3	0	C12	C11	3	See individual bit resets.	64-bit	Interrupt Controller Running Priority Register
ICV_RPR_EL1	3	0	C12	C11	3	See individual bit resets.	64-bit	Interrupt Controller Virtual Running Priority Register
ICC_SGI1R_EL1	3	0	C12	C11	5	See individual bit resets.	64-bit	Interrupt Controller Software Generated Interrupt Group 1 Register
ICC_ASGI1R_EL1	3	0	C12	C11	6	See individual bit resets.	64-bit	Interrupt Controller Alias Software Generated Interrupt Group 1 Register
ICC_SGI0R_EL1	3	0	C12	C11	7	See individual bit resets.	64-bit	Interrupt Controller Software Generated Interrupt Group 0 Register
ICC_IAR1_EL1	3	0	C12	C12	0	See individual bit resets.	64-bit	Interrupt Controller Interrupt Acknowledge Register 1
ICV_IAR1_EL1	3	0	C12	C12	0	See individual bit resets.	64-bit	Interrupt Controller Virtual Interrupt Acknowledge Register 1
ICC_EOIR1_EL1	3	0	C12	C12	1	See individual bit resets.	64-bit	Interrupt Controller End Of Interrupt Register 1
ICV_EOIR1_EL1	3	0	C12	C12	1	See individual bit resets.	64-bit	Interrupt Controller Virtual End Of Interrupt Register 1
ICC_HPPIR1_EL1	3	0	C12	C12	2	See individual bit resets.	64-bit	Interrupt Controller Highest Priority Pending Interrupt Register 1
ICV_HPPIR1_EL1	3	0	C12	C12	2	See individual bit resets.	64-bit	Interrupt Controller Virtual Highest Priority Pending Interrupt Register 1
ICC_BPR1_EL1	3	0	C12	C12	3	See individual bit resets.	64-bit	Interrupt Controller Binary Point Register 1
ICV_BPR1_EL1	3	0	C12	C12	3	See individual bit resets.	64-bit	Interrupt Controller Virtual Binary Point Register 1
ICC_CTLR_EL1	3	0	C12	C12	4	See individual bit resets.	64-bit	Interrupt Controller Control Register (EL1)
ICV_CTLR_EL1	3	0	C12	C12	4	See individual bit resets.	64-bit	Interrupt Controller Virtual Control Register
ICC_SRE_EL1	3	0	C12	C12	5	See individual bit resets.	64-bit	Interrupt Controller System Register Enable Register (EL1)
ICC_IGRPEN0_EL1	3	0	C12	C12	6	See individual bit resets.	64-bit	Interrupt Controller Interrupt Group 0 Enable register
ICV_IGRPEN0_EL1	3	0	C12	C12	6	See individual bit resets.	64-bit	Interrupt Controller Virtual Interrupt Group 0 Enable register



Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">ICC_IGRPEN1_EL1</a>	3	0	C12	C12	7	See individual bit resets.	64-bit	Interrupt Controller Interrupt Group 1 Enable register
<a href="#">ICV_IGRPEN1_EL1</a>	3	0	C12	C12	7	See individual bit resets.	64-bit	Interrupt Controller Virtual Interrupt Group 1 Enable register
<a href="#">ICH_LR&lt;n&gt;_EL2</a>	3	4	C12	110:m[3]	m[2:0]	See individual bit resets.	64-bit	Interrupt Controller List Registers
<a href="#">ICH_AP0R&lt;n&gt;_EL2</a>	3	4	C12	C8	0:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Hyp Active Priorities Group 0 Registers
<a href="#">ICH_AP1R&lt;n&gt;_EL2</a>	3	4	C12	C9	0:m[1:0]	See individual bit resets.	64-bit	Interrupt Controller Hyp Active Priorities Group 1 Registers
<a href="#">ICC_SRE_EL2</a>	3	4	C12	C9	5	See individual bit resets.	64-bit	Interrupt Controller System Register Enable Register (EL2)
<a href="#">ICH_HCR_EL2</a>	3	4	C12	C11	0	See individual bit resets.	64-bit	Interrupt Controller Hyp Control Register
<a href="#">ICH_VTR_EL2</a>	3	4	C12	C11	1	See individual bit resets.	64-bit	Interrupt Controller VGIC Type Register
<a href="#">ICH_MISR_EL2</a>	3	4	C12	C11	2	See individual bit resets.	64-bit	Interrupt Controller Maintenance Interrupt State Register
<a href="#">ICH_EISR_EL2</a>	3	4	C12	C11	3	See individual bit resets.	64-bit	Interrupt Controller End of Interrupt Status Register
<a href="#">ICH_ELSR_EL2</a>	3	4	C12	C11	5	See individual bit resets.	64-bit	Interrupt Controller Empty List Register Status Register
<a href="#">ICH_VMCR_EL2</a>	3	4	C12	C11	7	See individual bit resets.	64-bit	Interrupt Controller Virtual Machine Control Register

### A.1.7 AArch64 RAS registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** RAS registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-7: RAS registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">ERRIDR_EL1</a>	3	0	C5	C3	0	See individual bit resets.	64-bit	Error Record ID Register
<a href="#">ERRSELR_EL1</a>	3	0	C5	C3	1	See individual bit resets.	64-bit	Error Record Select Register
<a href="#">ERXFR_EL1</a>	3	0	C5	C4	0	See individual bit resets.	64-bit	Selected Error Record Feature Register
<a href="#">ERXCTLR_EL1</a>	3	0	C5	C4	1	See individual bit resets.	64-bit	Selected Error Record Control Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">ERXSTATUS_EL1</a>	3	0	C5	C4	2	See individual bit resets.	64-bit	Selected Error Record Primary Status Register
<a href="#">ERXADDR_EL1</a>	3	0	C5	C4	3	See individual bit resets.	64-bit	Selected Error Record Address Register
<a href="#">ERXPFGF_EL1</a>	3	0	C5	C4	4	See individual bit resets.	64-bit	Selected Pseudo-fault Generation Feature Register
<a href="#">ERXPFGCTL_EL1</a>	3	0	C5	C4	5	See individual bit resets.	64-bit	Selected Pseudo-fault Generation Control Register
<a href="#">ERXPFGCDN_EL1</a>	3	0	C5	C4	6	See individual bit resets.	64-bit	Selected Pseudo-fault Generation Countdown Register
<a href="#">ERXMISCO_EL1</a>	3	0	C5	C5	0	See individual bit resets.	64-bit	Selected Error Record Miscellaneous Register 0
<a href="#">ERXMISC1_EL1</a>	3	0	C5	C5	1	See individual bit resets.	64-bit	Selected Error Record Miscellaneous Register 1
<a href="#">ERXMISC2_EL1</a>	3	0	C5	C5	2	See individual bit resets.	64-bit	Selected Error Record Miscellaneous Register 2
<a href="#">ERXMISC3_EL1</a>	3	0	C5	C5	3	See individual bit resets.	64-bit	Selected Error Record Miscellaneous Register 3
<a href="#">DISR_EL1</a>	3	0	C12	C1	1	See individual bit resets.	64-bit	Deferred Interrupt Status Register
<a href="#">VSESR_EL2</a>	3	4	C5	C2	3	See individual bit resets.	64-bit	Virtual SError Exception Syndrome Register
<a href="#">VDISR_EL2</a>	3	4	C12	C1	1	See individual bit resets.	64-bit	Virtual Deferred Interrupt Status Register

### A.1.8 AArch64 Trace unit registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Trace unit registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-8: Trace unit registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">TRCSEQEVR&lt;n&gt;</a>	2	1	C0	00:m[1:0]	4	See individual bit resets.	64-bit	Sequencer State Transition Control Register <n>
<a href="#">TRCCNTRLDVR&lt;n&gt;</a>	2	1	C0	00:m[1:0]	5	See individual bit resets.	64-bit	Counter Reload Value Register <n>
<a href="#">TRCCNTCTLR&lt;n&gt;</a>	2	1	C0	01:m[1:0]	5	See individual bit resets.	64-bit	Counter Control Register <n>
<a href="#">TRCCNTVR&lt;n&gt;</a>	2	1	C0	10:m[1:0]	5	See individual bit resets.	64-bit	Counter Value Register <n>

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TRCTRACEIDR	2	1	C0	C0	1	See individual bit resets.	64-bit	Trace ID Register
TRCVICTLR	2	1	C0	C0	2	See individual bit resets.	64-bit	ViewInst Main Control Register
TRCIDR8	2	1	C0	C0	6	See individual bit resets.	64-bit	ID Register 8
TRCIMSPECO	2	1	C0	C0	7	See individual bit resets.	64-bit	IMP DEF Register 0
TRCPRGCTLR	2	1	C0	C1	0	See individual bit resets.	64-bit	Programming Control Register
TRCVIIECTLR	2	1	C0	C1	2	See individual bit resets.	64-bit	ViewInst Include/Exclude Control Register
TRCIDR9	2	1	C0	C1	6	See individual bit resets.	64-bit	ID Register 9
TRCVISSCTLR	2	1	C0	C2	2	See individual bit resets.	64-bit	ViewInst Start/Stop Control Register
TRCIDR10	2	1	C0	C2	6	See individual bit resets.	64-bit	ID Register 10
TRCSTATR	2	1	C0	C3	0	See individual bit resets.	64-bit	Trace Status Register
TRCIDR11	2	1	C0	C3	6	See individual bit resets.	64-bit	ID Register 11
TRCCONFIGR	2	1	C0	C4	0	See individual bit resets.	64-bit	Trace Configuration Register
TRCIDR12	2	1	C0	C4	6	See individual bit resets.	64-bit	ID Register 12
TRCIDR13	2	1	C0	C5	6	See individual bit resets.	64-bit	ID Register 13
TRCAUXCTLR	2	1	C0	C6	0	See individual bit resets.	64-bit	Auxillary Control Register
TRCSEQRSTEV	2	1	C0	C6	4	See individual bit resets.	64-bit	Sequencer Reset Control Register
TRCSEQSTR	2	1	C0	C7	4	See individual bit resets.	64-bit	Sequencer State Register
TRCEVENTCTLOR	2	1	C0	C8	0	See individual bit resets.	64-bit	Event Control 0 Register
TRCVDCTLR	2	1	C0	C8	2	See individual bit resets.	64-bit	ViewData Main Control Register
TRCEXTINSEL	2	1	C0	C8	4	See individual bit resets.	64-bit	External Input Select Register
TRCIDR0	2	1	C0	C8	7	See individual bit resets.	64-bit	ID Register 0
TRCEVENTCTL1R	2	1	C0	C9	0	See individual bit resets.	64-bit	Event Control 1 Register
TRCVDSACCTLR	2	1	C0	C9	2	See individual bit resets.	64-bit	ViewData Include/Exclude Single Address Comparator Control Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TRCIDR1	2	1	C0	C9	7	See individual bit resets.	64-bit	ID Register 1
TRCVDARCCTLR	2	1	C0	C10	2	See individual bit resets.	64-bit	ViewData Include/Exclude Address Range Comparator Control Register
TRCIDR2	2	1	C0	C10	7	See individual bit resets.	64-bit	ID Register 2
TRCSTALLCTLR	2	1	C0	C11	0	See individual bit resets.	64-bit	Stall Control Register
TRCIDR3	2	1	C0	C11	7	See individual bit resets.	64-bit	ID Register 3
TRCTSCTLR	2	1	C0	C12	0	See individual bit resets.	64-bit	Timestamp Control Register
TRCIDR4	2	1	C0	C12	7	See individual bit resets.	64-bit	ID Register 4
TRCSYNCPR	2	1	C0	C13	0	See individual bit resets.	64-bit	Synchronization Period Register
TRCIDR5	2	1	C0	C13	7	See individual bit resets.	64-bit	ID Register 5
TRCCCCTLR	2	1	C0	C14	0	See individual bit resets.	64-bit	Cycle Count Control Register
TRCIDR6	2	1	C0	C14	7	See individual bit resets.	64-bit	ID Register 6
TRCBCTLR	2	1	C0	C15	0	See individual bit resets.	64-bit	Branch Broadcast Control Register
TRCIDR7	2	1	C0	C15	7	See individual bit resets.	64-bit	ID Register 7
TRCSSCCR<n>	2	1	C1	0:m[2:0]	2	See individual bit resets.	64-bit	Single-shot Comparator Control Register <n>
TRCSSCSR<n>	2	1	C1	1:m[2:0]	2	See individual bit resets.	64-bit	Single-shot Comparator Control Status Register <n>
TRCOSLAR	2	1	C1	C0	4	See individual bit resets.	64-bit	Trace OS Lock Access Register
TRCOSLSR	2	1	C1	C1	4	See individual bit resets.	64-bit	Trace OS Lock Status Register
TRCRSCTLR<n>	2	1	C1	m[3:0]	00:m[4]	See individual bit resets.	64-bit	Resource Selection Control Register <n>
TRCDVCVR<n>	2	1	C2	m[1:0]:00	10:m[2]	See individual bit resets.	64-bit	Data Value Comparator Value Register <n>
TRCDVCMR<n>	2	1	C2	m[1:0]:00	11:m[2]	See individual bit resets.	64-bit	Data Value Comparator Mask Register <n>
TRCACVR<n>	2	1	C2	m[2:0]:0	00:m[3]	See individual bit resets.	64-bit	Address Comparator Value Register <n>
TRCACATR<n>	2	1	C2	m[2:0]:0	01:m[3]	See individual bit resets.	64-bit	Address Comparator Access Type Register <n>
TRCCIDCCTLR0	2	1	C3	C0	2	See individual bit resets.	64-bit	Context Identifier Comparator Control Register 0

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
TRCVMIDCCTLR0	2	1	C3	C2	2	See individual bit resets.	64-bit	Virtual Context Identifier Comparator Control Register 0
TRCCIDCVR<n>	2	1	C3	m[2:0]:0	0	See individual bit resets.	64-bit	Context Identifier Comparator Value Registers <n>
TRCVMIDCVR<n>	2	1	C3	m[2:0]:0	1	See individual bit resets.	64-bit	Virtual Context Identifier Comparator Value Register <n>
TRCDEVID	2	1	C7	C2	7	See individual bit resets.	64-bit	Device Configuration Register
TRCCCLAIMSET	2	1	C7	C8	6	See individual bit resets.	64-bit	Claim Tag Set Register
TRCCCLAIMCLR	2	1	C7	C9	6	See individual bit resets.	64-bit	Claim Tag Clear Register
TRCAUTHSTATUS	2	1	C7	C14	6	See individual bit resets.	64-bit	Authentication Status Register
TRCDEVARCH	2	1	C7	C15	6	See individual bit resets.	64-bit	Device Architecture Register

### A.1.9 AArch64 Special-purpose registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Special-purpose registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-9: Special-purpose registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
SPSR_EL1	3	0	C4	C0	0	See individual bit resets.	64-bit	Saved Program Status Register (EL1)
ELR_EL1	3	0	C4	C0	1	See individual bit resets.	64-bit	Exception Link Register (EL1)
SP_ELO	3	0	C4	C1	0	See individual bit resets.	64-bit	Stack Pointer (ELO)
DSPSR_ELO	3	3	C4	C5	0	See individual bit resets.	64-bit	Debug Saved Program Status Register
DLR_ELO	3	3	C4	C5	1	See individual bit resets.	64-bit	Debug Link Register
SPSR_EL2	3	4	C4	C0	0	See individual bit resets.	64-bit	Saved Program Status Register (EL2)
ELR_EL2	3	4	C4	C0	1	See individual bit resets.	64-bit	Exception Link Register (EL2)
SP_EL1	3	4	C4	C1	0	See individual bit resets.	64-bit	Stack Pointer (EL1)
SPSR_irq	3	4	C4	C3	0	See individual bit resets.	64-bit	Saved Program Status Register (IRQ mode)
SPSR_abt	3	4	C4	C3	1	See individual bit resets.	64-bit	Saved Program Status Register (Abort mode)
SPSR_und	3	4	C4	C3	2	See individual bit resets.	64-bit	Saved Program Status Register (Undefined mode)
SPSR_fiq	3	4	C4	C3	3	See individual bit resets.	64-bit	Saved Program Status Register (FIQ mode)

## A.1.10 AArch64 Generic Timer registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Generic Timer registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-10: Generic Timer registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">CNTKCTL_EL1</a>	3	0	C14	C1	0	See individual bit resets.	64-bit	Counter-timer Kernel Control Register
<a href="#">CNTFRQ_ELO</a>	3	3	C14	C0	0	See individual bit resets.	64-bit	Counter-timer Frequency Register
<a href="#">CNTPCT_ELO</a>	3	3	C14	C0	1	See individual bit resets.	64-bit	Counter-timer Physical Count Register
<a href="#">CNTVCT_ELO</a>	3	3	C14	C0	2	See individual bit resets.	64-bit	Counter-timer Virtual Count Register
<a href="#">CNTP_TVAL_ELO</a>	3	3	C14	C2	0	See individual bit resets.	64-bit	Counter-timer Physical Timer TimerValue Register
<a href="#">CNTP_CTL_ELO</a>	3	3	C14	C2	1	See individual bit resets.	64-bit	Counter-timer Physical Timer Control Register
<a href="#">CNTP_CVAL_ELO</a>	3	3	C14	C2	2	See individual bit resets.	64-bit	Counter-timer Physical Timer CompareValue Register
<a href="#">CNTV_TVAL_ELO</a>	3	3	C14	C3	0	See individual bit resets.	64-bit	Counter-timer Virtual Timer TimerValue Register
<a href="#">CNTV_CTL_ELO</a>	3	3	C14	C3	1	See individual bit resets.	64-bit	Counter-timer Virtual Timer Control Register
<a href="#">CNTV_CVAL_ELO</a>	3	3	C14	C3	2	See individual bit resets.	64-bit	Counter-timer Virtual Timer CompareValue Register
<a href="#">CNTVOFF_EL2</a>	3	4	C14	C0	3	See individual bit resets.	64-bit	Counter-timer Virtual Offset Register
<a href="#">CNTHCTL_EL2</a>	3	4	C14	C1	0	See individual bit resets.	64-bit	Counter-timer Hypervisor Control Register
<a href="#">CNTHPS_TVAL_EL2</a>	3	4	C14	C5	0	See individual bit resets.	64-bit	Counter-timer Secure Physical Timer TimerValue Register (EL2)
<a href="#">CNTHPS_CTL_EL2</a>	3	4	C14	C5	1	See individual bit resets.	64-bit	Counter-timer Secure Physical Timer Control Register (EL2)
<a href="#">CNTHPS_CVAL_EL2</a>	3	4	C14	C5	2	See individual bit resets.	64-bit	Counter-timer Secure Physical Timer CompareValue Register (EL2)

### A.1.11 AArch64 Other system control registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** Other system control registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table A-11: Other system control registers summary**

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
<a href="#">IMP_TESTRO_EL1</a>	3	0	C15	C2	1	See individual bit resets.	64-bit	STL Test Register 0
<a href="#">IMP_TESTR1_EL1</a>	3	0	C15	C2	2	See individual bit resets.	64-bit	STL Test Register 1
<a href="#">IMP_TESTR1KEY_EL1</a>	3	0	C15	C2	3	See individual bit resets.	64-bit	STL TESTR1 Write Key Register
<a href="#">IMP_LFSR_EL1</a>	3	0	C15	C2	4	See individual bit resets.	64-bit	STL LFSR Pseudo-random Value Register
<a href="#">IMP_FCTLR_EL1</a>	3	0	C15	C8	0	See individual bit resets.	64-bit	Fault Control Register
<a href="#">IMP_FPIR_EL1</a>	3	0	C15	C8	1	See individual bit resets.	64-bit	Fault Partition Identifier Register
<a href="#">IMP_FFMIR_EL1</a>	3	0	C15	C8	2	See individual bit resets.	64-bit	Fault Failure Mode Identification Register
<a href="#">IMP_TESTR2_EL1</a>	3	0	C15	C8	4	See individual bit resets.	64-bit	STL Test Register 2
<a href="#">IMP_PMCCTRL_EL1</a>	3	0	C15	C9	0	See individual bit resets.	64-bit	STL Main Control Register
<a href="#">IMP_PMCPCR_EL1</a>	3	0	C15	C9	1	See individual bit resets.	64-bit	STL Memory Control Register
<a href="#">IMP_PMCBER_EL1</a>	3	0	C15	C9	2	See individual bit resets.	64-bit	STL Byte Enable Register
<a href="#">IMP_PMCPCR_EL1</a>	3	0	C15	C9	3	See individual bit resets.	64-bit	STL Program Counter Register
<a href="#">IMP_PMCHIGHADDR_EL1</a>	3	0	C15	C9	4	See individual bit resets.	64-bit	STL High Address Register
<a href="#">IMP_PMCCADDR_EL1</a>	3	0	C15	C9	5	See individual bit resets.	64-bit	STL Column Address Register
<a href="#">IMP_PMCRAADDR_EL1</a>	3	0	C15	C9	6	See individual bit resets.	64-bit	STL Row Address register
<a href="#">IMP_PMCAR_EL1</a>	3	0	C15	C9	7	See individual bit resets.	64-bit	STL Array Register
<a href="#">IMP_PMCCLR_EL1</a>	3	0	C15	C11	7	See individual bit resets.	64-bit	STL Loop Counter Register

Name	Op0	Op1	CRn	CRm	Op2	Reset	Width	Description
IMP_PMCMDM<n>_EL1	3	0	C15	C11	m[2:0]	See individual bit resets.	64-bit	STL Data Mask, Fault Bitmap, and Data Registers
IMP_PMCXM<n>_EL1	3	0	C15	C12	m[2:0]	See individual bit resets.	64-bit	STL XOR Mask Registers
IMP_PMCPC<n>_EL1	3	0	C15	C13	m[2:0]	See individual bit resets.	64-bit	STL Program Registers
SCTLR_EL2	3	4	C1	C0	0	See individual bit resets.	64-bit	System Control Register (EL2)
HSTR_EL2	3	4	C1	C1	3	See individual bit resets.	64-bit	Hypervisor System Trap Register

## A.2 AArch64 register descriptions

This section includes the register descriptions for all the AArch64 registers in the Cortex®-R82AE processor.

### A.2.1 AArch64 Identification register description

This section includes the register descriptions for all Identification registers in the Cortex®-R82AE processor.

#### A.2.1.1 MIDR\_EL1, Main ID Register

Provides identification information for the PE, including an implementer code for the device and a device ID number.

##### Configurations

AArch64 register MIDR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.17 MIDR\\_EL1, Main ID Register](#) on page 1765 bits [31:0].

##### Attributes

##### Width

64

##### Functional group

Identification registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0100	0001	0000	1111	1101	0001	0100	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-1: AARCH64\_MIDR\_EL1 bit assignments

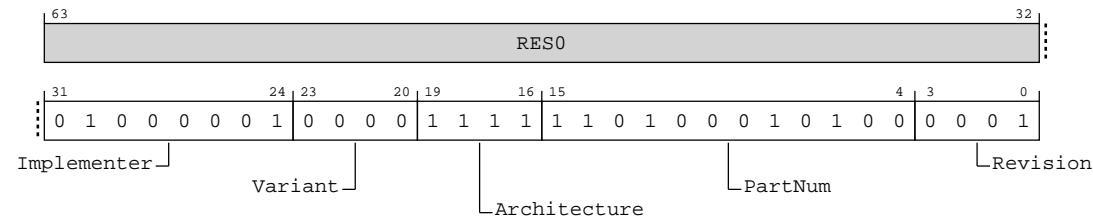


Table A-12: MIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:24]	Implementer	The Implementer code. This field must hold an implementer code that has been assigned by Arm. <b>0b01000001</b> Arm Limited	0x41
[23:20]	Variant	The major product revision variant number. <b>0b0000</b> r0.	0b0000
[19:16]	Architecture	Architecture version. Defined values are: <b>0b1111</b> Architectural features are individually identified in the ID_* registers. All other values are reserved.	0b1111
[15:4]	PartNum	The primary part number for the device. <b>0b110100010100</b> Cortex-R82AE.	0xD14
[3:0]	Revision	The minor product revision variant number. <b>0b0001</b> p1.	0b0001

Access

MRS <Xt>, MIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b000

Accessibility

MRS <Xt>, MIDR\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    X[t, 64] = VPIDR_EL2;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MIDR_EL1;
```

A.2.1.2 MPIDR\_EL1, Multiprocessor Affinity Register

In a multiprocessor system, provides an additional PE identification mechanism for scheduling purposes.

Configurations

In a uniprocessor system, Arm recommends that each Aff<n> field of this register returns a value of 0.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x0xx	xxx1	xxxx	xxxx	xxxx	xxxx	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-2: AARCH64\_MPIDR\_EL1 bit assignments

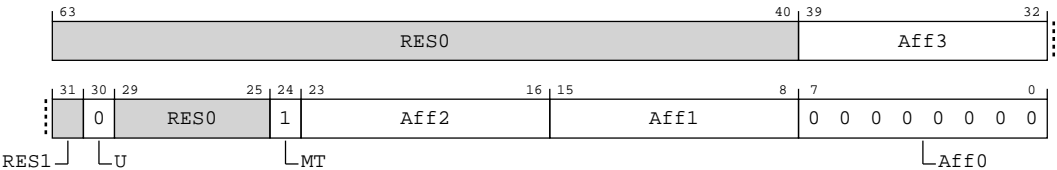


Table A-14: MPIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	Aff3	Affinity level 3. See the description of Aff0 for more information.  Value read from the CFGMPIDRAFF3 configuration pins.	8 {x}
[31]	RES1	Reserved	RES1
[30]	U	Indicates a Uniprocessor system, as distinct from PE 0 in a multiprocessor system.  <b>0b0</b>  Processor is part of a multiprocessor system.	0b0
[29:25]	RES0	Reserved	RES0
[24]	MT	Indicates whether the lowest level of affinity consists of logical PEs that are implemented using a multithreading type approach. See the description of Aff0 for more information about affinity levels.  <b>0b1</b>  Performance of PEs with different affinity level 0 values, and the same values for affinity level 1 and higher, is very interdependent.	0b1
[23:16]	Aff2	Affinity level 2. See the description of Aff0 for more information.  Value read from the CFGMPIDRAFF2 configuration pins.	8 {x}

Bits	Name	Description	Reset
[15:8]	Aff1	<p>Affinity level 1. See the description of Aff0 for more information.</p> <p><b>Note:</b> The value of this field refers to the index of logical cores. The number of logical cores implemented in the cluster are affected by AArch64-IMP_CLUSTERCFR_EL1.CEMODE.</p> <p><b>0b00000000</b> Core 0.</p> <p><b>0b00000001</b> Core 1.</p> <p><b>0b00000010</b> Core 2.</p> <p><b>0b00000011</b> Core 3.</p> <p><b>0b00000100</b> Core 4.</p> <p><b>0b00000101</b> Core 5.</p> <p><b>0b00000110</b> Core 6.</p> <p><b>0b00000111</b> Core 7.</p>	8{x}
[7:0]	Aff0	<p>Affinity level 0. This is the affinity level that is most significant for determining PE behavior. Higher affinity levels are increasingly less significant in determining PE behavior. The assigned value of the AArch64-MPIDR_EL1.{Aff3, Aff2, Aff1, Aff0} set of fields of each PE must be unique within the system as a whole.</p> <p><b>0b00000000</b> Single thread</p>	0x00

## Access

MRS <Xt>, MPIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b101

## Accessibility

MRS <Xt>, MPIDR\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    X[t, 64] = VMPIDR_EL2;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MPIDR_EL1;

```

A.2.1.3 REVIDR\_EL1, Revision ID Register

Provides implementation-specific minor revision information.

Configurations

This register is available in all configurations.

Attributes

Width

64

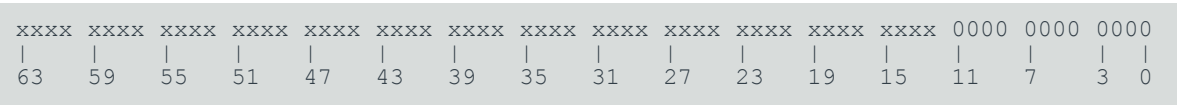
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-3: AARCH64\_REVIDR\_EL1 bit assignments

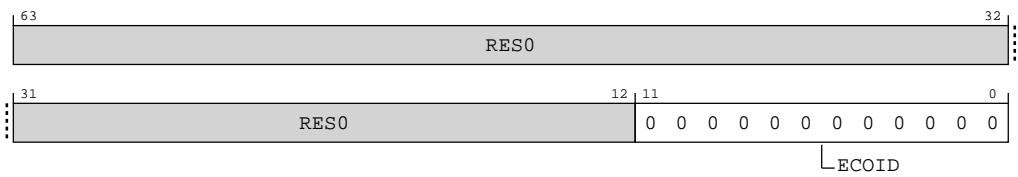


Table A-16: REVIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:12]	RES0	Reserved	RES0
[11:0]	ECOID	Contains information about the ECOs applied to this processor.  0b000000000000 No ECO applied.	0x000

Access

MRS <Xt>, REVIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b110

Accessibility

MRS <Xt>, REVIDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TID1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = REVIDR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = REVIDR_EL1;
```

A.2.1.4 ID\_PFR0\_EL1, AArch32 Processor Feature Register 0

Gives top-level information about the instruction sets supported by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_PFR1\_EL1.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

- Attributes
- Width
- 64
- Functional group
- Identification registers
- Access type
- See bit descriptions
- Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-4: AARCH64\_ID\_PFR0\_EL1 bit assignments

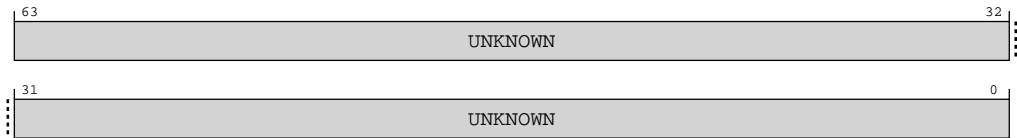


Table A-18: ID\_PFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_PFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b000

Accessibility

MRS <Xt>, ID\_PFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_PFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_PFR0_EL1;
```

A.2.1.5 ID\_PFR1\_EL1, AArch32 Processor Feature Register 1

Gives information about the AArch32 programmers' model.

Must be interpreted with AArch64-ID\_PFR0\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-5: AARCH64\_ID\_PFR1\_EL1 bit assignments

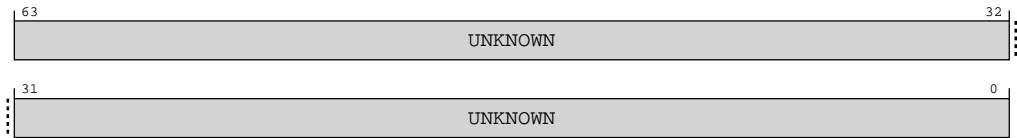


Table A-20: ID\_PFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_PFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b001

Accessibility

MRS <Xt>, ID\_PFR1\_EL1

```
if PSTATE.EL == EL0 then
```



```
if HCR_EL2.TGE == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    AArch64.SystemAccessTrap(EL1, 0x18);
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_PFR1_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ID_PFR1_EL1;
```

A.2.1.6 ID\_DFR0\_EL1, AArch32 Debug Feature Register 0

Provides top level information about the debug system in AArch32 state.

Must be interpreted with the Main ID Register, AArch64-MIDR\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-6: AARCH64\_ID\_DFR0\_EL1 bit assignments

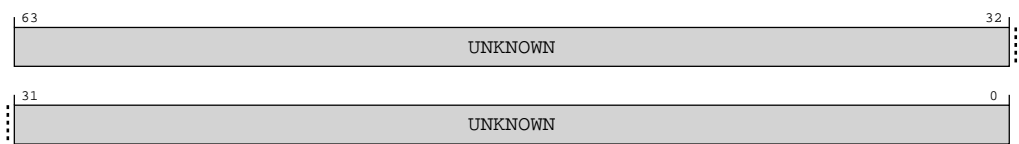


Table A-22: ID\_DFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_DFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b010

Accessibility

MRS <Xt>, ID\_DFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_DFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_DFR0_EL1;
```

A.2.1.7 ID\_AFR0\_EL1, AArch32 Auxiliary Feature Register 0

Provides information about the **IMPLEMENTATION DEFINED** features of the PE in AArch32 state.

Must be interpreted with the Main ID Register, AArch64-MIDR\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

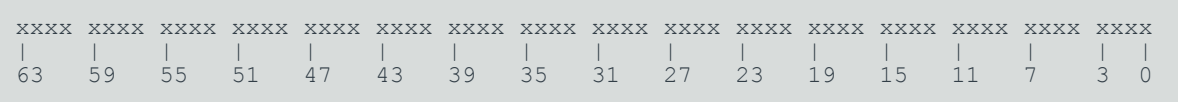
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-7: AARCH64\_ID\_AFR0\_EL1 bit assignments

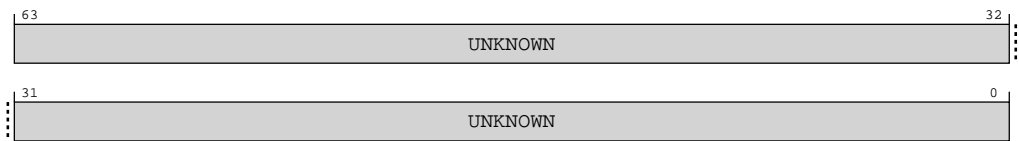


Table A-24: ID\_AFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_AFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b011

Accessibility

MRS <Xt>, ID\_AFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TID3 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = ID_AFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AFR0_EL1;
```

A.2.1.8 ID\_MMFR0\_EL1, AArch32 Memory Model Feature Register 0

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-8: AARCH64\_ID\_MMFR0\_EL1 bit assignments

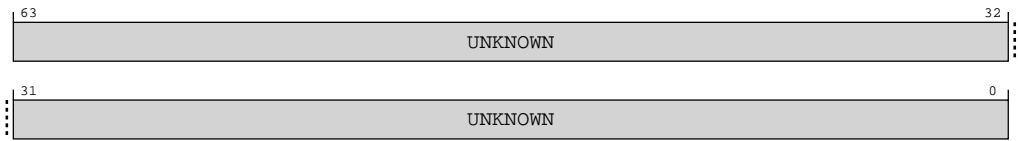


Table A-26: ID\_MMFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

**Access**  
MRS <Xt>, ID\_MMFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b100

**Accessibility**  
MRS <Xt>, ID\_MMFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR0_EL1;
```

A.2.1.9 ID\_MMFR1\_EL1, AArch32 Memory Model Feature Register 1

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Configurations**  
This register is available in all configurations.

**Attributes**

**Width**  
64

**Functional group**  
Identification registers

**Access type**  
See bit descriptions

**Reset value**

```
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
```



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-9: AARCH64\_ID\_MMFR1\_EL1 bit assignments

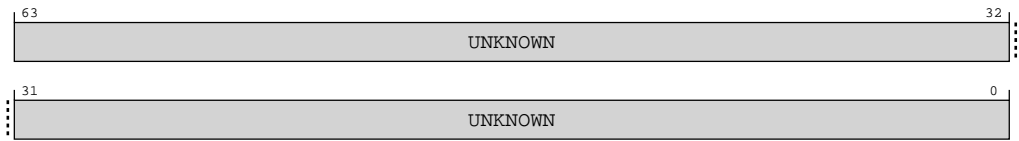


Table A-28: ID\_MMFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_MMFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b101

Accessibility

MRS <Xt>, ID\_MMFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR1_EL1;
```

A.2.1.10 ID\_MMFR2\_EL1, AArch32 Memory Model Feature Register 2

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

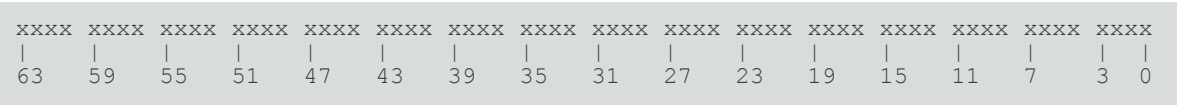
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-10: AARCH64\_ID\_MMFR2\_EL1 bit assignments

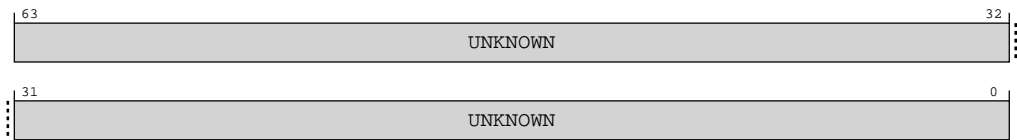


Table A-30: ID\_MMFR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_MMFR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b110

Accessibility

MRS <Xt>, ID\_MMFR2\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR2_EL1;
```

A.2.1.11 ID\_MMFR3\_EL1, AArch32 Memory Model Feature Register 3

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

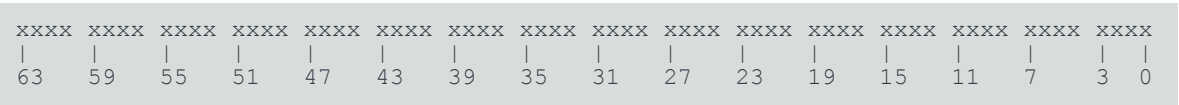
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-11: AARCH64\_ID\_MMFR3\_EL1 bit assignments

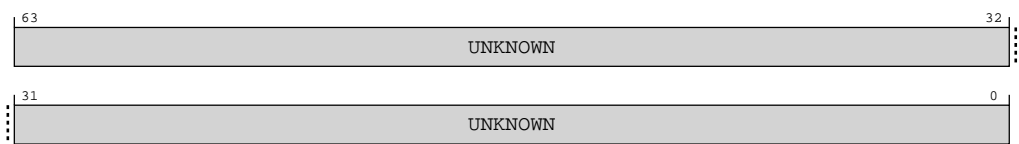


Table A-32: ID\_MMFR3\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_MMFR3\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0001	0b111

Accessibility

MRS <Xt>, ID\_MMFR3\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR3_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR3_EL1;
```

A.2.1.12 ID\_ISAR0\_EL1, AArch32 Instruction Set Attribute Register 0

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR3\_EL1, AArch64-ID\_ISAR4\_EL1, and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

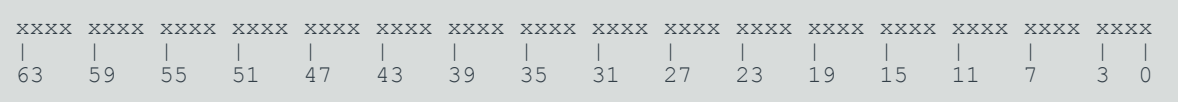
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-12: AARCH64\_ID\_ISARO\_EL1 bit assignments

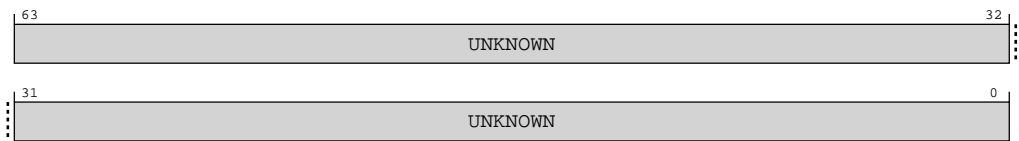


Table A-34: ID\_ISARO\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISARO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b000

Accessibility

MRS <Xt>, ID\_ISARO\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TID3 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = ID_ISAR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR0_EL1;
```

A.2.1.13 ID\_ISAR1\_EL1, AArch32 Instruction Set Attribute Register 1

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR3\_EL1, AArch64-ID\_ISAR4\_EL1, and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

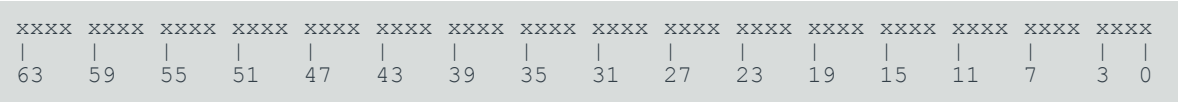
Functional group

Identification registers

Access type

See bit descriptions

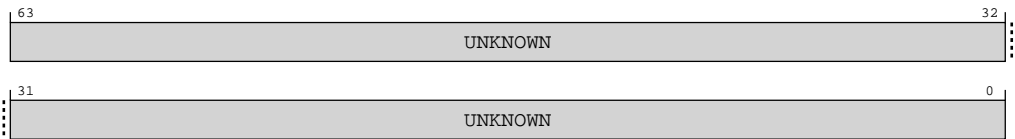
Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-13: AARCH64\_ID\_ISAR1\_EL1 bit assignments



**Table A-36: ID\_ISAR1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

**Access**

MRS &lt;Xt&gt;, ID\_ISAR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b001

**Accessibility**

MRS &lt;Xt&gt;, ID\_ISAR1\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_ISAR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR1_EL1;

```

**A.2.1.14 ID\_ISAR2\_EL1, AArch32 Instruction Set Attribute Register 2**

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR3\_EL1, AArch64-ID\_ISAR4\_EL1, and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Configurations**

This register is available in all configurations.

**Attributes****Width**

64

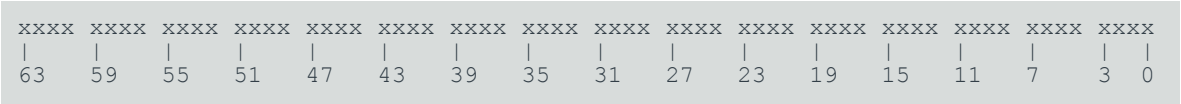
**Functional group**

Identification registers

**Access type**

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-14: AARCH64\_ID\_ISAR2\_EL1 bit assignments

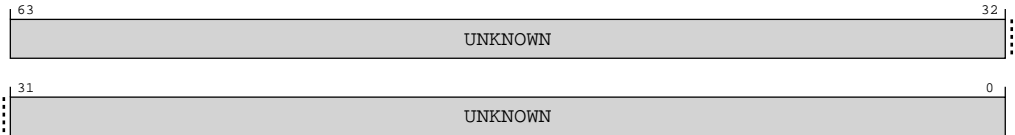


Table A-38: ID\_ISAR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISAR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b010

Accessibility

MRS <Xt>, ID\_ISAR2\_EL1

```
if PSTATE.EL == EL0 then
  if HCR_EL2.TGE == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
  if HCR_EL2.TID3 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    X[t, 64] = ID_ISAR2_EL1;
elseif PSTATE.EL == EL2 then
  X[t, 64] = ID_ISAR2_EL1;
```

A.2.1.15 ID\_ISAR3\_EL1, AArch32 Instruction Set Attribute Register 3

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR4\_EL1, and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

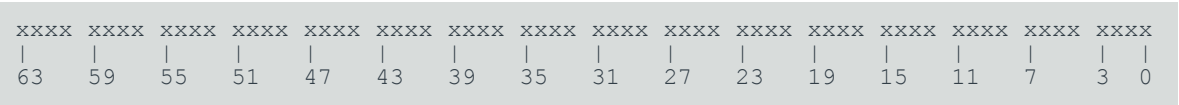
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-15: AARCH64\_ID\_ISAR3\_EL1 bit assignments

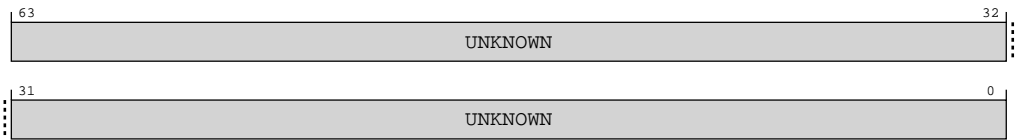


Table A-40: ID\_ISAR3\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISAR3\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b011

Accessibility

MRS <Xt>, ID\_ISAR3\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_ISAR3_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR3_EL1;
```

A.2.1.16 ID\_ISAR4\_EL1, AArch32 Instruction Set Attribute Register 4

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR3\_EL1, and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-16: AARCH64\_ID\_ISAR4\_EL1 bit assignments

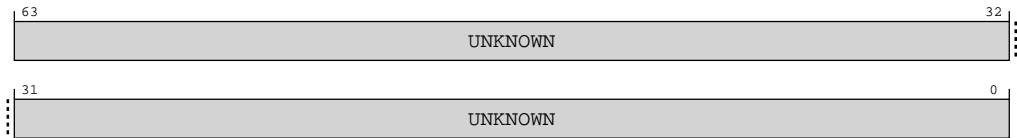


Table A-42: ID\_ISAR4\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISAR4\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b100

Accessibility

MRS <Xt>, ID\_ISAR4\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_ISAR4_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR4_EL1;
```

A.2.1.17 ID\_ISAR5\_EL1, AArch32 Instruction Set Attribute Register 5

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR3\_EL1, and AArch64-ID\_ISAR4\_EL1.



For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

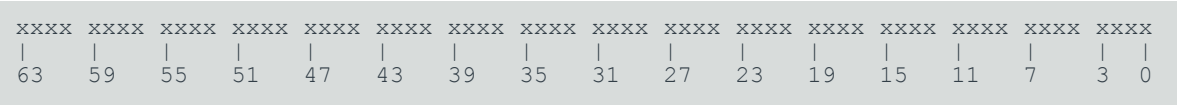
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-17: AARCH64\_ID\_ISAR5\_EL1 bit assignments

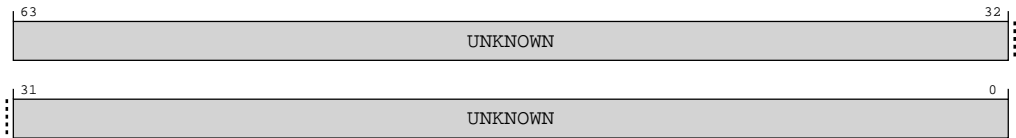


Table A-44: ID\_ISAR5\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISAR5\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b101

Accessibility

MRS <Xt>, ID\_ISAR5\_EL1


```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_ISAR5_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR5_EL1;
```

A.2.1.18 ID\_MMFR4\_EL1, AArch32 Memory Model Feature Register 4

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-18: AARCH64\_ID\_MMFR4\_EL1 bit assignments

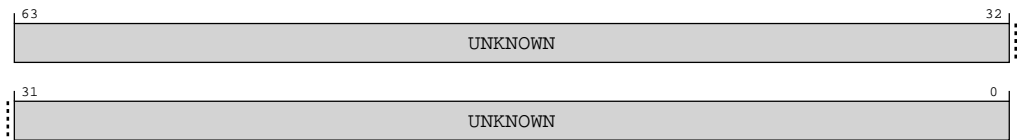


Table A-46: ID\_MMFR4\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_MMFR4\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b110

Accessibility

MRS <Xt>, ID\_MMFR4\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR4_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR4_EL1;
```

A.2.1.19 ID\_ISAR6\_EL1, AArch32 Instruction Set Attribute Register 6

Provides information about the instruction sets implemented by the PE in AArch32 state.

Must be interpreted with AArch64-ID\_ISAR0\_EL1, AArch64-ID\_ISAR1\_EL1, AArch64-ID\_ISAR2\_EL1, AArch64-ID\_ISAR3\_EL1, AArch64-ID\_ISAR4\_EL1 and AArch64-ID\_ISAR5\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

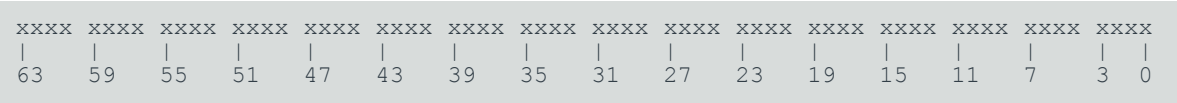
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-19: AARCH64\_ID\_ISAR6\_EL1 bit assignments

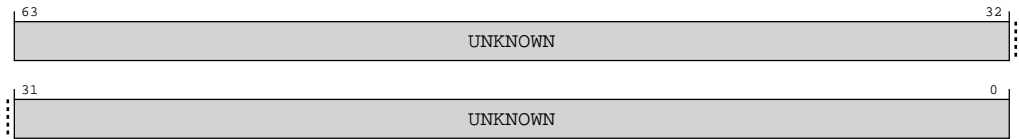


Table A-48: ID\_ISAR6\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_ISAR6\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0010	0b111

Accessibility

MRS <Xt>, ID\_ISAR6\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_ISAR6_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_ISAR6_EL1;
```

A.2.1.20 MVFR0\_EL1, AArch32 Media and VFP Feature Register 0

Describes the features provided by the AArch32 Advanced SIMD and Floating-point implementation.

Must be interpreted with AArch64-MVFR1\_EL1 and AArch64-MVFR2\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

In an implementation where at least one Exception level supports execution in AArch32 state, but there is no support for Advanced SIMD and floating-point operation, this register is RAZ.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-20: AARCH64\_MVFR0\_EL1 bit assignments

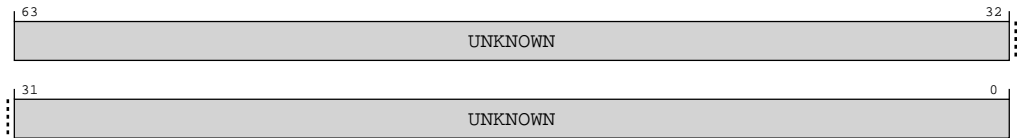


Table A-50: MVFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, MVFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b000

Accessibility

MRS <Xt>, MVFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MVFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MVFR0_EL1;
```

A.2.1.21 MVFR1\_EL1, AArch32 Media and VFP Feature Register 1

Describes the features provided by the AArch32 Advanced SIMD and Floating-point implementation.

Must be interpreted with AArch64-MVFR0\_EL1 and AArch64-MVFR2\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

In an implementation where at least one Exception level supports execution in AArch32 state, but there is no support for Advanced SIMD and floating-point operation, this register is RAZ.

Attributes

Width

64

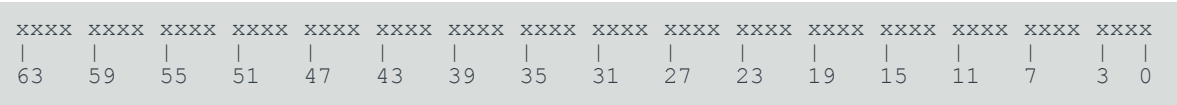
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-21: AARCH64\_MVFR1\_EL1 bit assignments

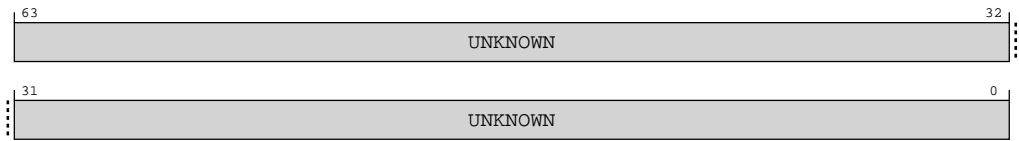


Table A-52: MVFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, MVFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b001

Accessibility

MRS <Xt>, MVFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MVFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MVFR1_EL1;
```

A.2.1.22 MVFR2\_EL1, AArch32 Media and VFP Feature Register 2

Describes the features provided by the AArch32 Advanced SIMD and Floating-point implementation.

Must be interpreted with AArch64-MVFR0\_EL1 and AArch64-MVFR1\_EL1.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

In an implementation where at least one Exception level supports execution in AArch32 state, but there is no support for Advanced SIMD and floating-point operation, this register is RAZ.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-22: AARCH64\_MVFR2\_EL1 bit assignments

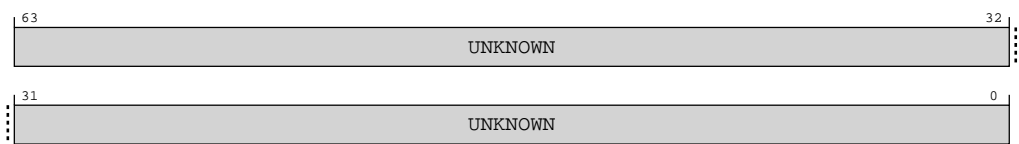


Table A-54: MVFR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, MVFR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b010

Accessibility

MRS <Xt>, MVFR2\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MVFR2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MVFR2_EL1;
```

A.2.1.23 ID\_PFR2\_EL1, AArch32 Processor Feature Register 2

Gives information about the AArch32 programmers' model.

Must be interpreted with AArch64-ID\_PFR0\_EL1 and AArch64-ID\_PFR1\_EL1.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

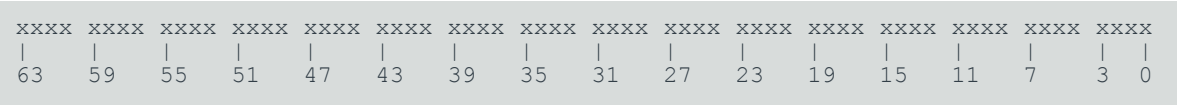
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-23: AARCH64\_ID\_PFR2\_EL1 bit assignments

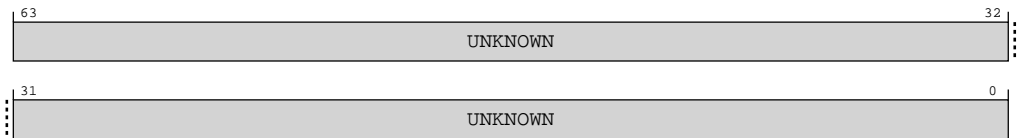


Table A-56: ID\_PFR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_PFR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b100

Accessibility

MRS <Xt>, ID\_PFR2\_EL1


```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if (!IsZero(ID_PFR2_EL1) || boolean IMPLEMENTATION_DEFINED "ID_PFR2_EL1 trapped
by HCR_EL2.TID3") && HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_PFR2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_PFR2_EL1;
```

A.2.1.24 ID\_DFR1\_EL1, Debug Feature Register 1

Provides top level information about the debug system in AArch32.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group


Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-24: AARCH64\_ID\_DFR1\_EL1 bit assignments

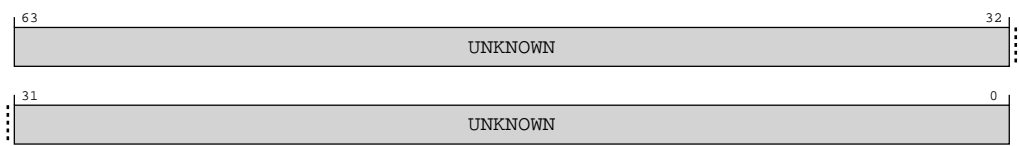


Table A-58: ID\_DFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_DFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b101

Accessibility

MRS <Xt>, ID\_DFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_DFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_DFR1_EL1;
```

A.2.1.25 ID\_MMFR5\_EL1, AArch32 Memory Model Feature Register 5

Provides information about the implemented memory model and memory management support in AArch32 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-25: AARCH64\_ID\_MMFR5\_EL1 bit assignments

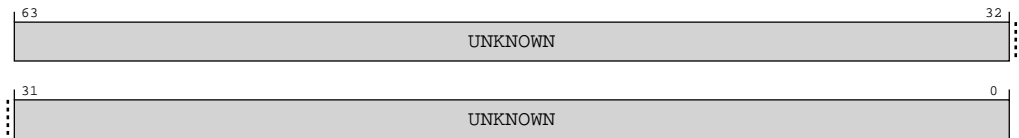


Table A-60: ID\_MMFR5\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

MRS <Xt>, ID\_MMFR5\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0011	0b110

Accessibility

MRS <Xt>, ID\_MMFR5\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_MMFR5_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_MMFR5_EL1;
```

A.2.1.26 ID\_AA64PFR0\_EL1, AArch64 Processor Feature Register 0

Provides additional information about implemented PE features in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

The external register ext-EDPFR gives information from this register.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

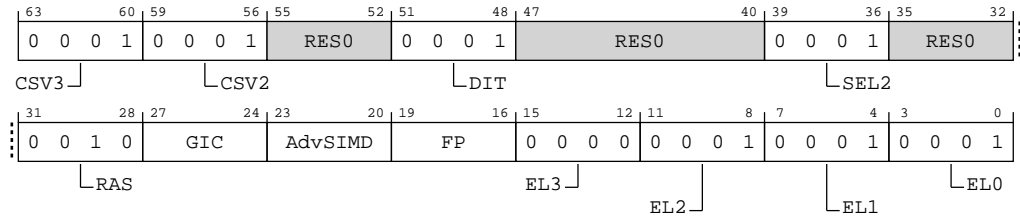
0001	0001	xxxx	0001	xxxx	xxxx	0001	xxxx	0010	xxxx	xxxx	xxxx	0000	0001	0001	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-26: AARCH64\_ID\_AA64PFR0\_EL1 bit assignments**



**Table A-62: ID\_AA64PFR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:60]	CSV3	Speculative use of faulting data. Defined values are: <b>0b0001</b> Data loaded under speculation with a permission or domain fault cannot be used to form an address, generate condition codes, or generate SVE predicate values to be used by other instructions in the speculative sequence. The execution timing of any other instructions in the speculative sequence is not a function of the data loaded under speculation.	0b0001
[59:56]	CSV2	Speculative use of out of context branch targets. Defined values are: <b>0b0001</b> FEAT_CSV2 is implemented, but FEAT_CSV2_2 and FEAT_CSV2_3 are not implemented.  AArch64-ID_AA64PFR1_EL1.CSV2_frac determines whether either or both of FEAT_CSV2_1p1 or FEAT_CSV2_1p2 are implemented.	0b0001
[55:52]	RES0	Reserved	RES0
[51:48]	DIT	Data Independent Timing. Defined values are: <b>0b0001</b> AArch64 provides the PSTATE.DIT mechanism to guarantee constant execution time of certain instructions.	0b0001
[47:40]	RES0	Reserved	RES0
[39:36]	SEL2	Secure EL2. Defined values are: <b>0b0001</b> Secure EL2 is implemented.	0b0001
[35:32]	RES0	Reserved	RES0
[31:28]	RAS	RAS Extension version. <b>0b0010</b> FEAT_RASv1p1 implemented. It also adds support for: <ul style="list-style-type: none"> <li>Additional ERXMISC&lt;m&gt;_EL1 System registers.</li> <li>Additional System registers AArch64-ERXPFGCDN_EL1, AArch64-ERXPFGCTL_EL1, and AArch64-ERXPFGF_EL1, and the AArch64-HCR_EL2.FIEN trap controls, to support the optional RAS Common Fault Injection Model Extension.</li> </ul> Error records accessed through System registers conform to RAS System Architecture v1.1, which includes simplifications to ext-ERR<n>STATUS and support for the optional RAS Timestamp and RAS Common Fault Injection Model Extensions.	0b0010

Bits	Name	Description	Reset
[27:24]	GIC	<p><b>When GICCDISABLE == 0</b> System register GIC interface support.</p> <p><b>0001</b> GIC CPU interface enabled. System register interface to versions 3.0 and 4.0 of the GIC CPU interface is supported.</p> <p><b>Otherwise</b> System register GIC interface support.</p> <p><b>0000</b> GIC CPU interface disabled. System register interface to any external GIC not supported.</p>	xxxx
[23:20]	AdvSIMD	<p><b>When NEON_FPm &gt; 0</b> Advanced SIMD.</p> <p><b>0001</b> Advanced SIMD is implemented that includes the FEAT_FP16 extension.</p> <p><b>Otherwise</b> Advanced SIMD.</p> <p><b>1111</b> Advanced SIMD is not implemented.</p>	xxxx
[19:16]	FP	<p><b>When NEON_FPm &gt; 0</b> Floating-point.</p> <p><b>0001</b> Floating-point is implemented that includes the FEAT_FP16 extension.</p> <p><b>Otherwise</b> Floating-point.</p> <p><b>1111</b> Floating-point is not implemented.</p>	xxxx
[15:12]	EL3	<p>EL3 Exception level handling.</p> <p><b>0b0000</b> EL3 is not implemented.</p>	0b0000
[11:8]	EL2	<p>EL2 Exception level handling.</p> <p><b>0b0001</b> EL2 can be executed in AArch64 state only.</p>	0b0001
[7:4]	EL1	<p>EL1 Exception level handling.</p> <p><b>0b0001</b> EL1 can be executed in AArch64 state only.</p>	0b0001
[3:0]	ELO	<p>ELO Exception level handling.</p> <p><b>0b0001</b> ELO can be executed in AArch64 state only.</p>	0b0001

## Access

MRS <Xt>, ID\_AA64PFR0\_EL1



op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0100	0b000

## Accessibility

MRS <Xt>, ID\_AA64PFR0\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64PFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64PFR0_EL1;

```

### A.2.1.27 ID\_AA64PFR1\_EL1, AArch64 Processor Feature Register 1

Reserved for future expansion of information about implemented PE features in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Identification registers

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0010	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-27: AARCH64\_ID\_AA64PFR1\_EL1 bit assignments

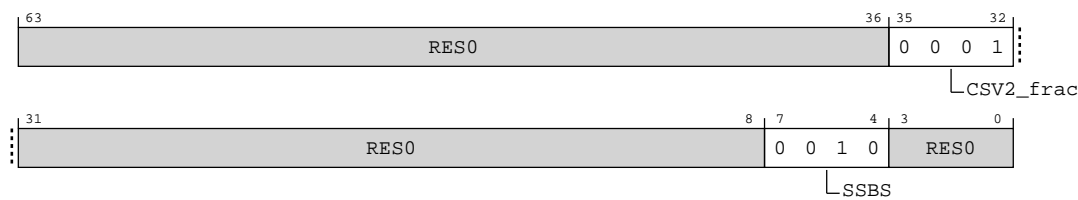


Table A-64: ID\_AA64PFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:36]	RES0	Reserved	RES0
[35:32]	CSV2_frac	CSV2 fractional field. Defined values are:  <b>0b0001</b> FEAT_CSV2_1p1 is implemented, but FEAT_CSV2_1p2 is not implemented.	0b0001
[31:8]	RES0	Reserved	RES0
[7:4]	SSBS	Speculative Store Bypassing controls in AArch64 state.  <b>0b0010</b> AArch64 provides the PSTATE.SSBS mechanism to mark regions that are Speculative Store Bypassing Safe, and the MSR and MRS instructions to directly read and write the PSTATE.SSBS field.	0b0010
[3:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID\_AA64PFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0100	0b001

Accessibility

MRS <Xt>, ID\_AA64PFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64PFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64PFR1_EL1;
```

A.2.1.28 ID\_AA64DFR0\_EL1, AArch64 Debug Feature Register 0

Provides top level information about the debug system in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

The external register ext-EDDFR gives information from this register.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	0001	1111	xxxx	0001	xxxx	0011	xxxx	0101	0101	0001	1001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-28: AARCH64\_ID\_AA64DFR0\_EL1 bit assignments

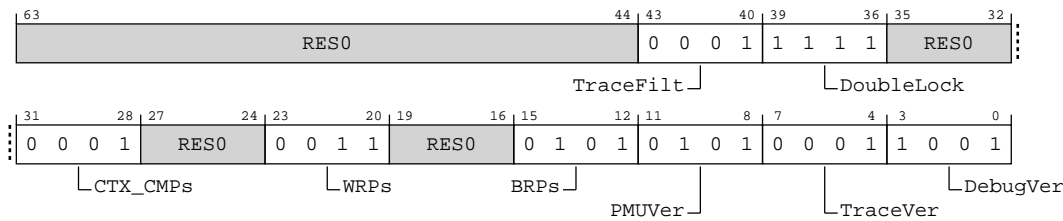


Table A-66: ID\_AA64DFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:44]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[43:40]	TraceFilt	Armv8.4 Self-hosted Trace Extension version. Defined values are:  <b>0b0001</b> Armv8.4 Self-hosted Trace Extension implemented.	0b0001
[39:36]	DoubleLock	OS Double Lock implemented. Defined values are:  <b>0b1111</b> OS Double Lock not implemented. AArch64-OSDLR_EL1 is <b>RAZ/WI</b> .	0b1111
[35:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:28]	CTX_CMPs	Number of breakpoints that are context-aware, minus 1.  <b>0b0001</b> 2 context-aware breakpoints implemented.  The value of this field is never greater than ID_AA64DFR0_EL1.BRPs.	0b0001
[27:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:20]	WRPs	Number of watchpoints, minus 1.  <b>0b0011</b> 4 watchpoints implemented.  The value of 0b0000 is reserved.	0b0011
[19:16]	<b>RES0</b>	Reserved	<b>RES0</b>
[15:12]	BRPs	Number of breakpoints, minus 1.  <b>0b0101</b> 6 breakpoints implemented.  The value of 0b0000 is reserved.	0b0101
[11:8]	PMUVer	Performance Monitors Extension version.  This field does not follow the standard ID scheme, but uses the alternative ID scheme described in <i>Alternative ID scheme used for the Performance Monitors Extension version</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>  Defined values are:  <b>0b0101</b> PMUv3 for Armv8.4. As 0b0100, and adds support for the AArch64-PM MIR_EL1 register.	0b0101
[7:4]	TraceVer	Trace support. Indicates whether System register interface to a trace unit is implemented. Defined values are:  <b>0b0001</b> Trace unit System registers implemented.	0b0001
[3:0]	DebugVer	Debug architecture version. Indicates presence of Armv8 debug architecture. Defined values are:  <b>0b1001</b> Armv8.4 debug architecture, FEAT_Debugv8p4.	0b1001

## Access

MRS <Xt>, ID\_AA64DFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0101	0b000

Accessibility

MRS <Xt>, ID\_AA64DFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64DFR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64DFR0_EL1;
```

A.2.1.29 ID\_AA64DFR1\_EL1, AArch64 Debug Feature Register 1

Provides top level information about the debug system in AArch64.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-29: AARCH64\_ID\_AA64DFR1\_EL1 bit assignments

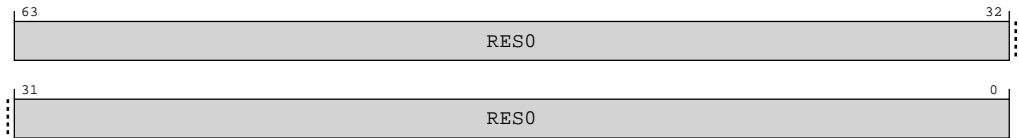


Table A-68: ID\_AA64DFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID\_AA64DFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0101	0b001

Accessibility

MRS <Xt>, ID\_AA64DFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64DFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64DFR1_EL1;
```

A.2.1.30 ID\_AA64AFR0\_EL1, AArch64 Auxiliary Feature Register 0

Provides information about the **IMPLEMENTATION DEFINED** features of the PE in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

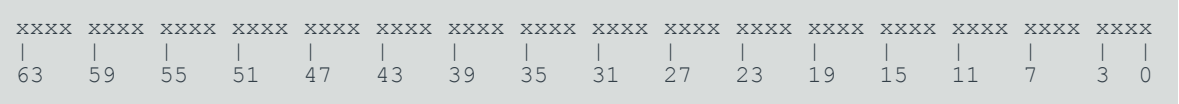
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-30: AARCH64\_ID\_AA64AFR0\_EL1 bit assignments

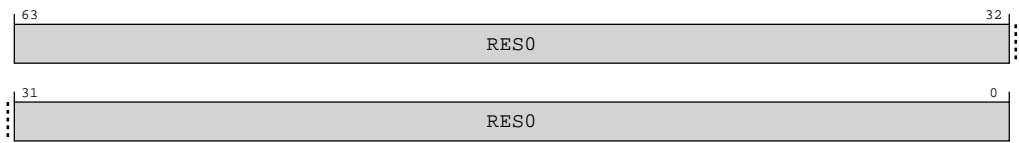


Table A-70: ID\_AA64AFR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID\_AA64AFR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0101	0b100

Accessibility

MRS <Xt>, ID\_AA64AFR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TID3 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = ID_AA64AFR0_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64AFR0_EL1;
```

A.2.1.31 ID\_AA64AFR1\_EL1, AArch64 Auxiliary Feature Register 1

Reserved for future expansion of information about the **IMPLEMENTATION DEFINED** features of the PE in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-31: AARCH64\_ID\_AA64AFR1\_EL1 bit assignments

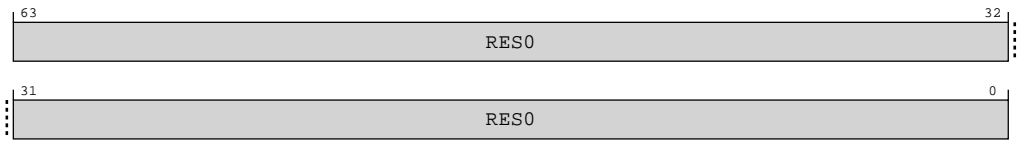




Table A-72: ID\_AA64AFR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

**Access**  
MRS <Xt>, ID\_AA64AFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0101	0b101

**Accessibility**  
MRS <Xt>, ID\_AA64AFR1\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64AFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64AFR1_EL1;
```

A.2.1.32 ID\_AA64ISAR0\_EL1, AArch64 Instruction Set Attribute Register 0

Provides information about the instructions implemented in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Configurations**  
This register is available in all configurations.

- Attributes**
- Width**  
64
- Functional group**  
Identification registers
- Access type**  
See bit descriptions
- Reset value**



63 59 55 51 47 43 39 35 31 27 23 19 15 11 7 3 0

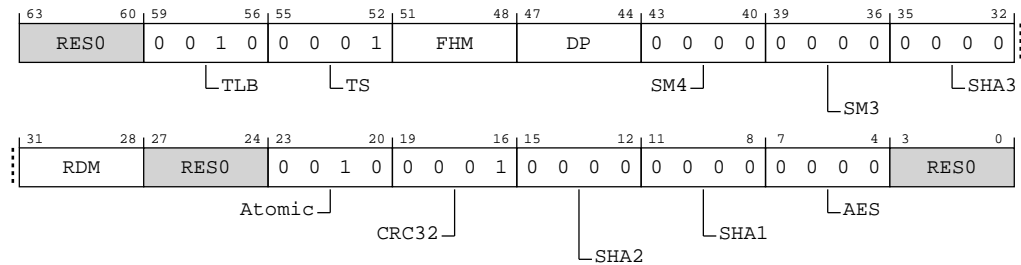


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-32: AARCH64\_ID\_AA64ISAR0\_EL1 bit assignments**



**Table A-74: ID\_AA64ISAR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:60]	RES0	Reserved	RES0
[59:56]	TLB	Indicates support for Outer Shareable and TLB range maintenance instructions. Defined values are: <b>0b0010</b> Outer Shareable and TLB range maintenance instructions are implemented.	0b0010
[55:52]	TS	Indicates support for flag manipulation instructions. Defined values are: <b>0b0001</b> CFINV, RMIF, SETF16, and SETF8 instructions are implemented.	0b0001
[51:48]	FHM	<b>When NEON_FPm &gt; 0</b> Indicates whether FMLAL and FMLSL instructions are implemented. <b>0001</b> FMLAL and FMLSL instructions are implemented.  <b>Otherwise</b> Indicates whether FMLAL and FMLSL instructions are implemented. <b>0000</b> FMLAL and FMLSL instructions are not implemented.	xxxx

Bits	Name	Description	Reset
[47:44]	DP	<b>When NEON_FPm &gt; 0</b> Dot Product instructions implemented. <b>0001</b> UDOT and SDOT instructions implemented.  <b>Otherwise</b> Dot Product instructions implemented. <b>0000</b> No Dot Product instructions implemented.	xxxx
[43:40]	SM4	Indicates support for SM4 instructions in AArch64 state. Defined values are: <b>0b0000</b> No SM4 instructions implemented.	0b0000
[39:36]	SM3	Indicates support for SM3 instructions in AArch64 state. Defined values are: <b>0b0000</b> No SM3 instructions implemented.	0b0000
[35:32]	SHA3	Indicates support for SHA3 instructions in AArch64 state. Defined values are: <b>0b0000</b> No SHA3 instructions implemented.	0b0000
[31:28]	RDM	<b>When NEON_FPm &gt; 0</b> SQRDMLAH and SQRDMLSH instructions implemented. <b>0001</b> SQRDMLAH and SQRDMLSH instructions implemented.  <b>Otherwise</b> SQRDMLAH and SQRDMLSH instructions implemented. <b>0000</b> No SQRDMLAH and SQRDMLSH instructions implemented.	xxxx
[27:24]	RES0	Reserved	RES0
[23:20]	Atomic	Indicates support for Atomic instructions in AArch64 state. Defined values are: <b>0b0010</b> LDADD, LDCLR, LDEOR, LDSET, LDSMAX, LDSMIN, LDUMAX, LDUMIN, CAS, CASP, and SWP instructions implemented.	0b0010
[19:16]	CRC32	Indicates support for CRC32 instructions in AArch64 state. Defined values are: <b>0b0001</b> CRC32B, CRC32H, CRC32W, CRC32X, CRC32CB, CRC32CH, CRC32CW, and CRC32CX instructions are implemented.	0b0001
[15:12]	SHA2	Indicates support for SHA2 instructions in AArch64 state. Defined values are: <b>0b0000</b> No SHA2 instructions implemented.	0b0000
[11:8]	SHA1	Indicates support for SHA1 instructions in AArch64 state. Defined values are: <b>0b0000</b> No SHA1 instructions implemented.	0b0000

Bits	Name	Description	Reset
[7:4]	AES	Indicates support for AES instructions in AArch64 state. Defined values are:  <b>0b0000</b> No AES instructions implemented.	0b0000
[3:0]	RES0	Reserved	RES0

**Access**  
MRS <Xt>, ID\_AA64ISAR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0110	0b000

**Accessibility**  
MRS <Xt>, ID\_AA64ISAR0\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64ISAR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64ISAR0_EL1;
```

A.2.1.33 ID\_AA64ISAR1\_EL1, AArch64 Instruction Set Attribute Register 1

Provides information about the features and instructions implemented in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Configurations**  
This register is available in all configurations.

- Attributes**
- Width**  
64
  - Functional group**  
Identification registers
  - Access type**  
See bit descriptions

## Reset value

xxxx	xxxx	xxxx	0001	xxxx	0001	0001	xxxx	0000	0000	0010	xxxx	xxxx	0000	0000	0010
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-33: AARCH64\_ID\_AA64ISAR1\_EL1 bit assignments

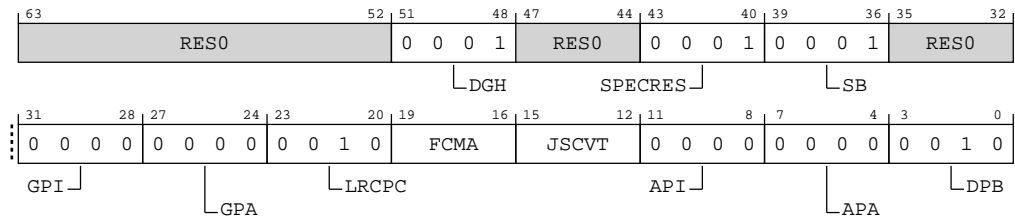


Table A-76: ID\_AA64ISAR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:52]	RES0	Reserved	RES0
[51:48]	DGH	Indicates support for the Data Gathering Hint instruction. Defined values are: <b>0b0001</b> Data Gathering Hint is implemented.	0b0001
[47:44]	RES0	Reserved	RES0
[43:40]	SPECRES	Indicates support for prediction invalidation instructions in AArch64 state. Defined values are: <b>0b0001</b> CFP RCTX, DVP RCTX and CPP RCTX instructions are implemented.	0b0001
[39:36]	SB	Indicates support for SB instruction in AArch64 state. Defined values are: <b>0b0001</b> SB instruction is implemented.	0b0001
[35:32]	RES0	Reserved	RES0
[31:28]	GPI	Indicates support for an <b>IMPLEMENTATION DEFINED</b> algorithm is implemented in the PE for generic code authentication in AArch64 state. Defined values are: <b>0b0000</b> Generic Authentication using an <b>IMPLEMENTATION DEFINED</b> algorithm is not implemented.	0b0000
[27:24]	GPA	Indicates whether the QARMA5 algorithm is implemented in the PE for generic code authentication in AArch64 state. <b>0b0000</b> Generic Authentication using the QARMA5 algorithm is not implemented.	0b0000

Bits	Name	Description	Reset
[23:20]	LRCPC	Indicates support for weaker release consistency, RCpc, based model. Defined values are:  <b>0b0010</b> As 0b0001, and the LDAPR (unscaled immediate) and STLR (unscaled immediate) instructions are implemented.	0b0010
[19:16]	FCMA	<b>When NEON_FPM &gt; 0</b> Indicates support for complex number addition and multiplication, where numbers are stored in vectors.  <b>0001</b> The FCMLA and FCADD instructions are implemented.  <b>Otherwise</b> Indicates support for complex number addition and multiplication, where numbers are stored in vectors.  <b>0000</b> The FCMLA and FCADD instructions are not implemented.	xxxx
[15:12]	JSCVT	<b>When NEON_FPM &gt; 0</b> Indicates support for javascript conversion from double precision floating point values to integers.  <b>0001</b> The FJCVTZS instruction is implemented.  <b>Otherwise</b> Indicates support for javascript conversion from double precision floating point values to integers.  <b>0000</b> The FJCVTZS instruction is not implemented.	xxxx
[11:8]	API	Indicates whether an <b>IMPLEMENTATION DEFINED</b> algorithm is implemented in the PE for address authentication, in AArch64 state. This applies to all Pointer Authentication instructions other than the <b>PACGA</b> instruction. Defined values are:  <b>0b0000</b> Address Authentication using an <b>IMPLEMENTATION DEFINED</b> algorithm is not implemented.	0b0000
[7:4]	APA	Indicates whether the QARMA5 algorithm is implemented in the PE for address authentication, in AArch64 state. This applies to all Pointer Authentication instructions other than the <b>PACGA</b> instruction.  <b>0b0000</b> Address Authentication using the QARMA5 algorithm is not implemented.	0b0000
[3:0]	DPB	Data Persistence writeback. Indicates support for the DC CVAP and DC CVADP instructions in AArch64 state. Defined values are:  <b>0b0010</b> DC CVAP and DC CVADP supported.	0b0010

## Access

MRS <Xt>, ID\_AA64ISAR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0110	0b001

Accessibility

MRS <Xt>, ID\_AA64ISAR1\_EL1


```
if PSTATE.EL == EL0 then
  if HCR_EL2.TGE == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    AArch64.SystemAccessTrap(EL1, 0x18);
elsif PSTATE.EL == EL1 then
  if HCR_EL2.TID3 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    X[t, 64] = ID_AA64ISAR1_EL1;
elsif PSTATE.EL == EL2 then
  X[t, 64] = ID_AA64ISAR1_EL1;
```

A.2.1.34 ID\_AA64ISAR2\_EL1, AArch64 Instruction Set Attribute Register 2

Provides information about the features and instructions implemented in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group


Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	xxxx	xxxx	0101	0001	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-34: AARCH64\_ID\_AA64ISAR2\_EL1 bit assignments

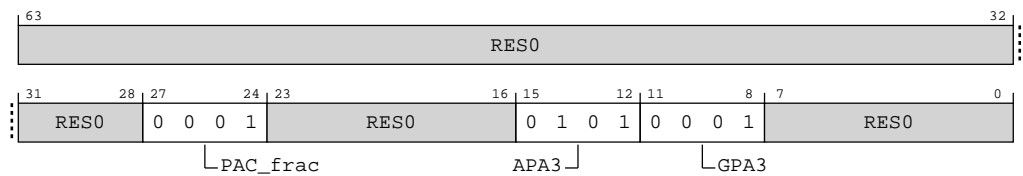


Table A-78: ID\_AA64ISAR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:28]	RES0	Reserved	RES0
[27:24]	PAC_frac	Indicates whether the ConstPACField() function used as part of the PAC addition returns FALSE or TRUE.  0b0001 ConstPACField() returns TRUE.	0b0001
[23:16]	RES0	Reserved	RES0
[15:12]	APA3	Indicates whether the QARMA3 algorithm is implemented in the PE for address authentication in AArch64 state. This applies to all Pointer Authentication instructions other than the PACGA instruction.  0b0101 Address Authentication using the QARMA3 algorithm is implemented, with the HaveEnhancedPAC2() function returning TRUE, the HaveFPAC() function returning TRUE, the HaveFPACCombined() function returning TRUE, and the HaveEnhancedPAC() function returning FALSE.	0b0101
[11:8]	GPA3	Indicates whether the QARMA3 algorithm is implemented in the PE for generic code authentication in AArch64 state.  0b0001 Generic Authentication using the QARMA3 algorithm is implemented. This includes the PACGA instruction.	0b0001
[7:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID\_AA64ISAR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0110	0b010

Accessibility

MRS <Xt>, ID\_AA64ISAR2\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if (!IsZero(ID_AA64ISAR2_EL1) || boolean IMPLEMENTATION_DEFINED
        "ID_AA64ISAR2_EL1_trapped by HCR_EL2.TID3") && HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```



```
        X[t, 64] = ID_AA64ISAR2_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ID_AA64ISAR2_EL1;
```

A.2.1.35 ID\_AA64MMFR0\_EL1, AArch64 Memory Model Feature Register 0

Provides information about the implemented memory model and memory management support in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

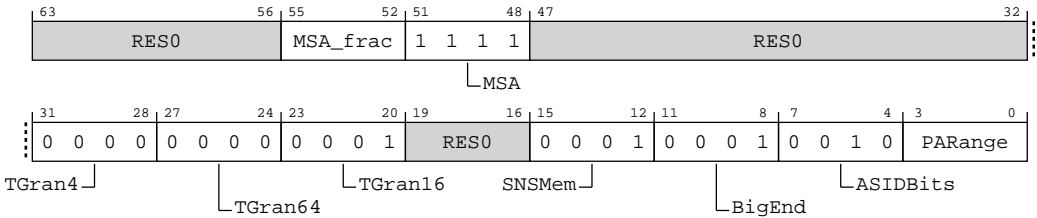
xxxx	xxxx	xxxx	1111	xxxx	xxxx	xxxx	xxxx	0000	0000	0001	xxxx	0001	0001	0010	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-35: AARCH64\_ID\_AA64MMFR0\_EL1 bit assignments



**Table A-80: ID\_AA64MMFR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:52]	MSA_frac	<p><b>When VMSAm == 1</b></p> <p>Memory System Architecture fractional field. This holds information on additional Memory System Architectures supported.</p> <p><b>0010</b></p> <p>PMSAv8-64 supported in all translation regimes. In addition to PMSAv8-64, stage 1 EL1&amp;0 transaltion regime also supports VMSAv8-64.</p> <p><b>Otherwise</b></p> <p>Memory System Architecture fractional field. This holds information on additional Memory System Architectures supported.</p> <p><b>0001</b></p> <p>PMSAv8-64 supported in all translation regimes. VMSAv8-64 not supported.</p>	xxxx
[51:48]	MSA	<p>Memory System Architecture ID field. This holds the information on Memory System Architectures supported. Defined values are:</p> <p><b>0b1111</b></p> <p>See ID_AA64MMFR0_EL1.MSA_frac for the Memory System Architectures supported.</p>	0b1111
[47:32]	RES0	Reserved	RES0
[31:28]	TGran4	<p>Indicates support for 4KB memory translation granule size. Defined values are:</p> <p><b>0b0000</b></p> <p>4KB granule supported.</p>	0b0000
[27:24]	TGran64	<p>Indicates support for 64KB memory translation granule size. Defined values are:</p> <p><b>0b0000</b></p> <p>64KB granule supported.</p>	0b0000
[23:20]	TGran16	<p>Indicates support for 16KB memory translation granule size. Defined values are:</p> <p><b>0b0001</b></p> <p>16KB granule supported.</p>	0b0001
[19:16]	RES0	Reserved	RES0
[15:12]	SNSMem	<p>Indicates support for a distinction between Secure and Non-secure Memory. Defined values are:</p> <p><b>0b0001</b></p> <p>Does support a distinction between Secure and Non-secure Memory.</p>	0b0001
[11:8]	BigEnd	<p>Indicates support for mixed-endian configuration. Defined values are:</p> <p><b>0b0001</b></p> <p>Mixed-endian support. The SCTLR_ELx.EE and AArch64-SCTLR_EL1.E0E bits can be configured.</p>	0b0001
[7:4]	ASIDBits	<p>Number of ASID bits. Defined values are:</p> <p><b>0b0010</b></p> <p>16 bits.</p>	0b0010

Bits	Name	Description	Reset
[3:0]	PARange	<p><b>When PA_W == 48</b> Physical Address range supported.</p> <p><b>0101</b> 48 bits, 256TB.</p> <p><b>Otherwise</b> Physical Address range supported.</p> <p><b>0010</b> 40 bits, 1TB.</p>	xxxx

### Access

MRS &lt;Xt&gt;, ID\_AA64MMFRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0111	0b000

### Accessibility

MRS &lt;Xt&gt;, ID\_AA64MMFRO\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64MMFRO_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64MMFRO_EL1;

```

## A.2.1.36 ID\_AA64MMFR1\_EL1, AArch64 Memory Model Feature Register 1

Provides information about the implemented memory model and memory management support in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

**Functional group**

Identification registers

**Access type**

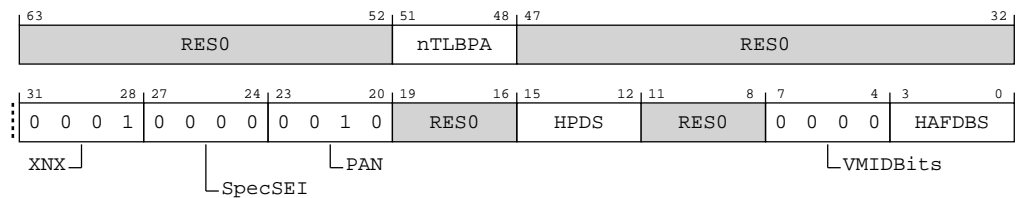
See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0000	0010	xxxx	xxxx	xxxx	0000	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-36: AARCH64\_ID\_AA64MMFR1\_EL1 bit assignments****Table A-82: ID\_AA64MMFR1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:52]	RES0	Reserved	RES0
[51:48]	nTLBPA	<b>When VMSAm == 1</b> Indicates support for intermediate caching of translation table walks. <b>0001</b> The intermediate caching of translation table walks does not include non-coherent caches of previous valid translation table entries since the last completed TLBI applicable to the PE where either: <ul style="list-style-type: none"> <li>The caching is indexed by the physical address of the location holding the translation table entry.</li> <li>The caching is used for stage 1 translations and is indexed by the intermediate physical address of the location holding the translation table entry.</li> </ul> <b>Otherwise</b> RES0	xxxx
[47:32]	RES0	Reserved	RES0
[31:28]	XNX	Indicates support for execute-never control distinction by Exception level at stage 2. Defined values are: <b>0b0001</b> Distinction between EL0 and EL1 execute-never control at stage 2 supported.	0b0001

Bits	Name	Description	Reset
[27:24]	SpecSEI	Describes whether the PE can generate SError interrupt exceptions from speculative reads of memory, including speculative instruction fetches.  <b>0b0000</b> The PE never generates an SError interrupt due to an External abort on a speculative read.	0b0000
[23:20]	PAN	Privileged Access Never. Indicates support for the PAN bit in PSTATE, AArch64-SPSR_EL1, AArch64-SPSR_EL2, and AArch64-DSPSR_ELO. Defined values are:  <b>0b0010</b> PAN supported and AT S1E1RP and AT S1E1WP instructions supported.	0b0010
[19:16]	RES0	Reserved	RES0
[15:12]	HPDS	<b>When VMSAm == 1</b> Hierarchical permission disables bits in translation tables.  <b>0001</b> Disabling of hierarchical controls supported with the AArch64-TCR_EL1.{HPD1, HPD0} bits.  <b>Otherwise</b> Hierarchical permission disables bits in translation tables.  <b>0000</b> Disabling of hierarchical controls not supported.	xxxx
[11:8]	RES0	Reserved	RES0
[7:4]	VMIDBits	Number of VMID bits. Defined values are:  <b>0b0000</b> 8 bits	0b0000
[3:0]	HAFDBS	<b>When VMSAm == 1</b> Hardware updates to Access flag and Dirty state in translation tables.  <b>0001</b> Hardware update of the Access flag is supported.  <b>Otherwise</b> Hardware updates to Access flag and Dirty state in translation tables.  <b>0000</b> Hardware update of the Access flag and dirty state are not supported.	xxxx

## Access

MRS <Xt>, ID\_AA64MMFR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0111	0b001

## Accessibility

MRS <Xt>, ID\_AA64MMFR1\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);

```


```
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64MMFR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64MMFR1_EL1;
```

A.2.1.37 ID\_AA64MMFR2\_EL1, AArch64 Memory Model Feature Register 2

Provides information about the implemented memory model and memory management support in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

  
Note

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group


Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	0001	0001	0001	xxxx	xxxx	0000	xxxx	0001	xxxx	0001	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

  
Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-37: AARCH64\_ID\_AA64MMFR2\_EL1 bit assignments

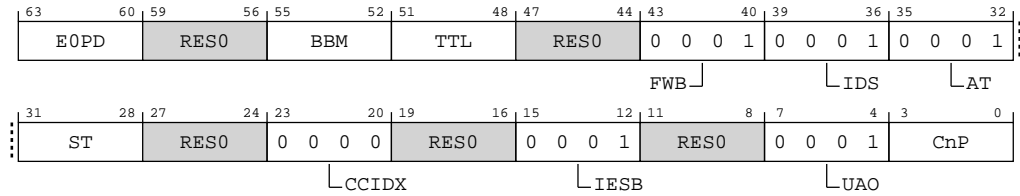


Table A-84: ID\_AA64MMFR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:60]	EOPD	<b>When VMSAm == 1</b> Indicates support for the FEAT_EOPD mechanism. <b>0001</b> EOPDx mechanism is implemented.  <b>Otherwise</b> Indicates support for the FEAT_EOPD mechanism. <b>0000</b> EOPDx mechanism is not implemented.	xxxx
[59:56]	RES0	Reserved	RES0
[55:52]	BBM	<b>When VMSAm == 1</b> Allows identification of the requirements of the hardware to have break-before-make sequences when changing block size for a translation. <b>0001</b> Level 1 support for changing block size is supported.  <b>Otherwise</b> Allows identification of the requirements of the hardware to have break-before-make sequences when changing block size for a translation. <b>0000</b> Level 0 support for changing block size is supported.	xxxx
[51:48]	TTL	<b>When VMSAm == 1</b> Indicates support for TTL field in address operations. <b>0001</b> TLB maintenance instructions by address have bits[47:44] holding the TTL field.  <b>Otherwise</b> Indicates support for TTL field in address operations. <b>0000</b> TLB maintenance instructions by address have bits[47:44] as RES0.	xxxx
[47:44]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[43:40]	FWB	Indicates support for AArch64-HCR_EL2.FWB. Defined values are:  <b>0b0001</b> AArch64-HCR_EL2.FWB is supported.	0b0001
[39:36]	IDS	Indicates the value of ESR_ELx.EC that reports an exception generated by a read access to the feature ID space. Defined values are:  <b>0b0001</b> All exceptions generated by an AArch64 read access to the feature ID space are reported by ESR_ELx.EC == 0x18.  The Feature ID space is defined as the System register space in AArch64 with op0==3, op1=={0, 1, 3}, CRn==0, CRm=={0-7}, op2=={0-7}.	0b0001
[35:32]	AT	Identifies support for unaligned single-copy atomicity and atomic functions. Defined values are:  <b>0b0001</b> Unaligned single-copy atomicity and atomic functions with a 16-byte address range aligned to 16-bytes are supported.	0b0001
[31:28]	ST	<b>When VMSAm == 1</b> Identifies support for small translation tables.  <b>0001</b> The maximum value of the TCR_ELx.{TOSZ,T1SZ} and VTCR_EL2.TOSZ fields is 48 for 4KB and 16KB granules, and 47 for 64KB granules.  <b>Otherwise</b> Identifies support for small translation tables.  <b>0000</b> The maximum value of the TCR_ELx.{TOSZ,T1SZ} and VTCR_EL2.TOSZ fields is 39.	xxxx
[27:24]	RES0	Reserved	RES0
[23:20]	CCIDX	Support for the use of revised AArch64-CCSIDR_EL1 register format. Defined values are:  <b>0b0000</b> 32-bit format implemented for all levels of the CCSIDR_EL1.	0b0000
[19:16]	RES0	Reserved	RES0
[15:12]	IESB	Indicates support for the IESB bit in the SCTLR_ELx registers. Defined values are:  <b>0b0001</b> IESB bit in the SCTLR_ELx registers is supported.	0b0001
[11:8]	RES0	Reserved	RES0
[7:4]	UAO	User Access Override. Defined values are:  <b>0b0001</b> UAO supported.	0b0001



Bits	Name	Description	Reset
[3:0]	CnP	<b>When VMSAm == 1</b> Common not Private translations. <b>0001</b> Common not Private translations supported.  <b>Otherwise</b> Common not Private translations. <b>0000</b> Common not Private translations not supported.	xxxx

Access

MRS <Xt>, ID\_AA64MMFR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0111	0b010

Accessibility


MRS <Xt>, ID\_AA64MMFR2\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64MMFR2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64MMFR2_EL1;
```

A.2.1.38 ID\_AA64MMFR3\_EL1, AArch64 Memory Model Feature Register 3

Provides information about the implemented memory model and memory management support in AArch64 state.

Configurations



**Note**

Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-38: AARCH64\_ID\_AA64MMFR3\_EL1 bit assignments

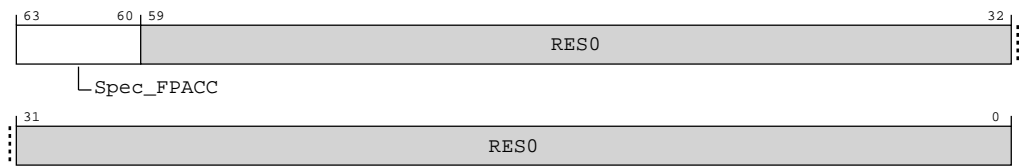


Table A-86: ID\_AA64MMFR3\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:60]	Spec_FPACC	Speculative behavior in the event of a PAC authentication failure in an implementation that includes FEAT_FPACCOMBINE. Defined values are:  <b>0b0001</b> The speculative use of pointers processed by a PAC Authentication is not materially different in terms of the impact on cached microarchitectural state between passing and failing of the PAC Authentication.  All other values are reserved.  For the purpose of this definition, cached microarchitecture state is the state of caching agents such as instruction caches, data caches and TLBs which can be altered as a result of speculation caused by a mispredicted execution, but is not restored to the state prior to the speculation when the misprediction is corrected.	xxxx
[59:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID\_AA64MMFR3\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0111	0b011

Accessibility

MRS <Xt>, ID\_AA64MMFR3\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ID_AA64MMFR3_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ID_AA64MMFR3_EL1;
```

A.2.1.39 CCSIDR\_EL1, Current Cache Size ID Register

Provides information about the architecture of the currently selected cache.

Configurations

The implementation includes one CCSIDR\_EL1 for each cache that it can access. AArch64-CSSELR\_EL1 selects which Cache Size ID Register is accessible.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

When AArch64-CSSELR\_EL1.Level == '000' and AArch64-CSSELR\_EL1.InD == '0'

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxx0 0000 0001 1010

When AArch64-CSSELR\_EL1.Level == '000' and AArch64-CSSELR\_EL1.InD == '1'

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxx0 0000 0001 1010

When L2\_CACHE\_SIZE > 0, AArch64-CSSELR\_EL1.Level == '001' and AArch64-CSSELR\_EL1.InD == '0'

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxx0 0000 0001 1010

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When AArch64-CSSELR\_EL1.Level == '000' and AArch64-CSSELR\_EL1.InD == '0'

Figure A-39: AARCH64\_CCSIDR\_EL1 bit assignments

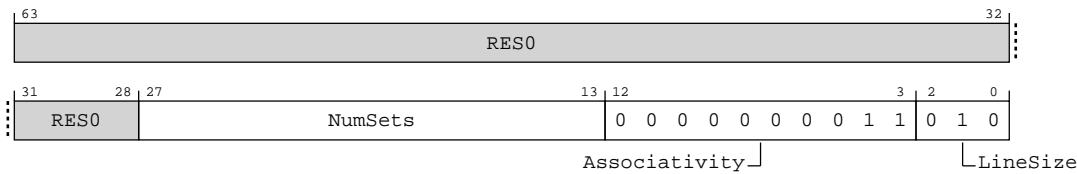


Table A-88: CCSIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:28]	RES0	Reserved	RES0
[27:13]	NumSets	(Number of sets in cache) - 1.  0b0000000001111111 64 sets.  0b0000000011111111 128 sets.  0b0000000111111111 256 sets.	15{x}
[12:3]	Associativity	(Associativity of cache) - 1.  0b0000000011 4 cache lines per set.	0b0000000011
[2:0]	LineSize	(Log <sub>2</sub> (Number of bytes in cache line)) - 4.  0b010 64 bytes per cache line.	0b010

When AArch64-CSSELR\_EL1.Level == '000' and AArch64-CSSELR\_EL1.InD == '1'

Figure A-40: AARCH64\_CCSIDR\_EL1 bit assignments

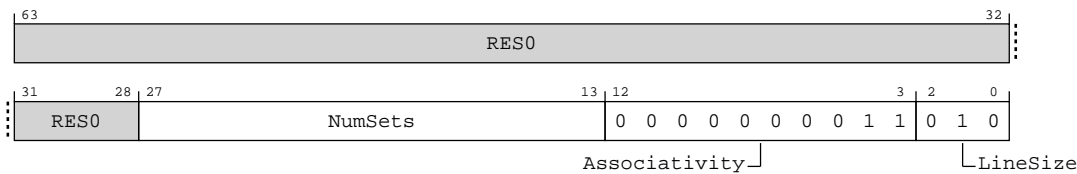


Table A-89: CCSIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:28]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[27:13]	NumSets	(Number of sets in cache) - 1.  <b>0b000000000111111</b> 64 sets.  <b>0b000000001111111</b> 128 sets.  <b>0b000000011111111</b> 256 sets.  <b>0b000000111111111</b> 512 sets.	15{x}
[12:3]	Associativity	(Associativity of cache) - 1.  <b>0b0000000011</b> 4 cache lines per set.	0b0000000011
[2:0]	LineSize	(Log <sub>2</sub> (Number of bytes in cache line)) - 4.  <b>0b010</b> 64 bytes per cache line.	0b010

When L2\_CACHE\_SIZE > 0, AArch64-CSSELR\_EL1.Level == '001' and AArch64-CSSELR\_EL1.InD == '0'

Figure A-41: AARCH64\_CCSDR\_EL1 bit assignments

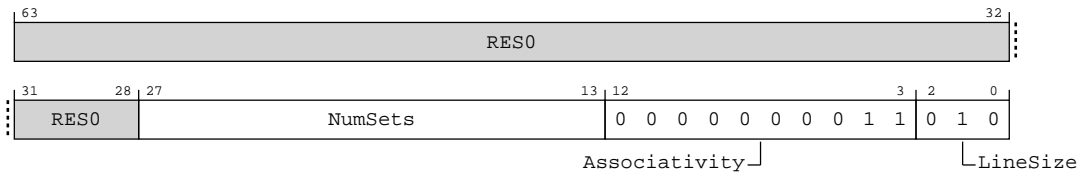


Table A-90: CCSIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:28]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[27:13]	NumSets	(Number of sets in cache) - 1.  <b>0b0000000101111111</b> 192 sets.  <b>0b0000000111111111</b> 256 sets.  <b>0b0000001011111111</b> 384 sets.  <b>0b0000001111111111</b> 512 sets.  <b>0b0000010111111111</b> 768 sets.  <b>0b0000011111111111</b> 1024 sets.  <b>0b0000101111111111</b> 1536 sets.  <b>0b0000111111111111</b> 2048 sets.  <b>0b0001011111111111</b> 3072 sets.  <b>0b0001111111111111</b> 4096 sets.  <b>0b0010111111111111</b> 6144 sets.  <b>0b0011111111111111</b> 8192 sets.	15{x}
[12:3]	Associativity	(Associativity of cache) - 1.  <b>0b0000000011</b> 4 cache lines per set.	0b0000000011
[2:0]	LineSize	(Log <sub>2</sub> (Number of bytes in cache line)) - 4.  <b>0b010</b> 64 bytes per cache line.	0b010

Figure A-42: AARCH64\_CCSIDR\_EL1 bit assignments

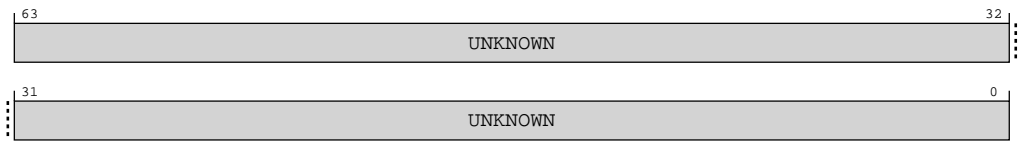


Table A-91: CCSIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

If AArch64-CSSELR\_EL1.{Level, InD} is programmed to a cache level that is not implemented, then on a read of the CCSIDR\_EL1 the behavior is **CONSTRAINED UNPREDICTABLE**, and can be one of the following:

- The CCSIDR\_EL1 read returns an **UNKNOWN** value.

MRS <Xt>, CCSIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b001	0b0000	0b0000	0b000

Accessibility

If AArch64-CSSELR\_EL1.{Level, InD} is programmed to a cache level that is not implemented, then on a read of the CCSIDR\_EL1 the behavior is **CONSTRAINED UNPREDICTABLE**, and can be one of the following:

- The CCSIDR\_EL1 read returns an **UNKNOWN** value.

MRS <Xt>, CCSIDR\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CCSIDR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CCSIDR_EL1;
```

A.2.1.40 CLIDR\_EL1, Cache Level ID Register

Identifies the type of cache, or caches, that are implemented at each level and can be managed using the architected cache maintenance instructions that operate by set/way, up to a maximum of seven levels. Also identifies the Level of Coherence (LoC) and Level of Unification (LoU) for the cache hierarchy.

Configurations

This register is available in all configurations.

Attributes

Width

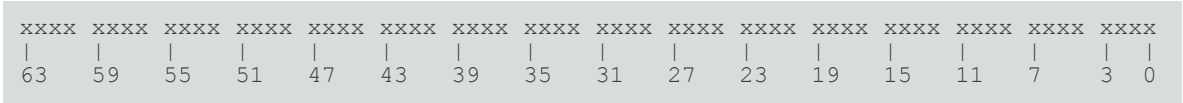
64

Functional group

Identification registers

Access type  
See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-43: AARCH64\_CLIDR\_EL1 bit assignments

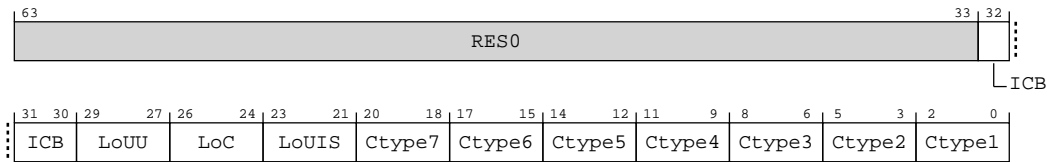


Table A-93: CLIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:33]	RES0	Reserved	RES0
[32:30]	ICB	<div><b>When L2_CACHE_SIZE &gt; 0</b> Inner cache boundary. This field indicates the boundary for caching Inner Cacheable memory regions. <b>010</b> L2 cache is the highest Inner Cacheable level.</div> <div><b>Otherwise</b> Inner cache boundary. This field indicates the boundary for caching Inner Cacheable memory regions. <b>001</b> L1 cache is the highest Inner Cacheable level.</div>	xxx



Bits	Name	Description	Reset
[29:27]	LoUU	<p>Level of Unification Uniprocessor for the cache hierarchy.</p> <p>For a description of the values of this field, see Terminology for Clean, Invalidate, and Clean and Invalidate instructions.</p> <p><b>Note:</b> This field does not describe the requirements for instruction cache invalidation. See AArch64-CTR_ELO.DIC.</p> <p><b>Note:</b> When FEAT_S2FWB is implemented, the architecture requires that this field is zero so that no levels of data cache need to be cleaned in order to manage coherency with instruction fetches.</p> <p><b>0b000</b> Level of Unification Uniprocessor is before the L1 cache.</p>	xxx
[26:24]	LoC	<p><b>When L2_CACHE_SIZE &gt; 0</b> Level of Coherence for the cache hierarchy.</p> <p><b>010</b> L2 cache is the level of coherence.</p> <p><b>Otherwise</b> Level of Coherence for the cache hierarchy.</p> <p><b>001</b> L1 cache is the level of coherence.</p>	xxx
[23:21]	LoUIS	<p>Level of Unification Inner Shareable for the cache hierarchy.</p> <p>For a description of the values of this field, see Terminology for Clean, Invalidate, and Clean and Invalidate instructions.</p> <p><b>Note:</b> This field does not describe the requirements for instruction cache invalidation. See AArch64-CTR_ELO.DIC.</p> <p><b>Note:</b> When FEAT_S2FWB is implemented, the architecture requires that this field is zero so that no levels of data cache need to be cleaned in order to manage coherency with instruction fetches.</p> <p><b>0b000</b> Level of Unification Inner Shareable is before the L1 cache.</p>	xxx
[20:18]	Ctype7	<p>Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:</p> <p><b>0b000</b> No cache.</p>	xxx
[17:15]	Ctype6	<p>Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:</p> <p><b>0b000</b> No cache.</p>	xxx

Bits	Name	Description	Reset
[14:12]	Ctype5	Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:  <b>0b000</b> No cache.	xxx
[11:9]	Ctype4	Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:  <b>0b000</b> No cache.	xxx
[8:6]	Ctype3	Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:  <b>0b000</b> No cache.  All other values are reserved.  If software reads the Cache Type fields from Ctype1 upwards, once it has seen a value of 000, no caches that can be managed using the architected cache maintenance instructions that operate by set/way exist at further-out levels of the hierarchy. So, for example, if Ctype3 is the first Cache Type field with a value of 000, the values of Ctype4 to Ctype7 must be ignored.	xxx
[5:3]	Ctype2	<b>When L2_CACHE_SIZE &gt; 0</b> Cache Type at level 2. <b>100</b> Unified cache at L2.  <b>Otherwise</b> Cache Type at level 2. <b>000</b> No cache at L2.	xxx
[2:0]	Ctype1	Cache Type fields. Indicate the type of cache that is implemented and can be managed using the architected cache maintenance instructions that operate by set/way at each level, from Level 1 up to a maximum of seven levels of cache hierarchy. Possible values of each field are:  <b>0b011</b> Separate instruction and data caches.	xxx

## Access

MRS &lt;Xt&gt;, CLIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b001	0b0000	0b0000	0b001

## Accessibility

MRS &lt;Xt&gt;, CLIDR\_EL1

```
if PSTATE.EL == EL0 then
```

```
if HCR_EL2.TGE == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    AArch64.SystemAccessTrap(EL1, 0x18);
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CLIDR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = CLIDR_EL1;
```

A.2.1.41 CSSELR\_EL1, Cache Size Selection Register

Selects the current Cache Size ID Register, AArch64-CCSIDR\_EL1, by specifying the required cache level and the cache type (either instruction or data cache).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

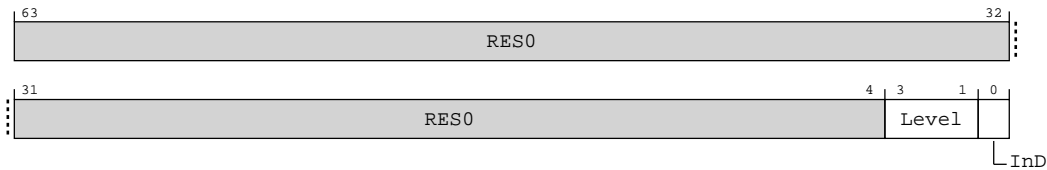


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-44: AARCH64\_CSSELR\_EL1 bit assignments



**Table A-95: CSSELR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:1]	Level	<p>Cache level of required cache.</p> <p><b>0b000</b> Level 1 cache.</p> <p><b>0b001</b> Level 2 cache.</p> <p><b>0b010</b> Level 3 cache.</p> <p><b>0b011</b> Level 4 cache.</p> <p><b>0b100</b> Level 5 cache.</p> <p><b>0b101</b> Level 6 cache.</p> <p><b>0b110</b> Level 7 cache.</p> <p>All other values are reserved.</p> <p>If CSSELR_EL1.{Level, InD} is programmed to a cache level that is not implemented, then the value for this field on a read of CSSELR_EL1 is <b>UNKNOWN</b>.</p>	xxx
[0]	InD	<p>Instruction not Data bit.</p> <p><b>0b0</b> Data or unified cache.</p> <p><b>0b1</b> Instruction cache.</p> <p>If CSSELR_EL1.{Level, InD} is programmed to a cache level that is not implemented, then a read of CSSELR_EL1 is CONSTRAINED UNPREDICTABLE, and returns <b>UNKNOWN</b> values for CSSELR_EL1.{Level, InD}.</p>	x

**Access**

MRS &lt;Xt&gt;, CSSELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b0000	0b0000	0b000

MSR CSSELR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b010	0b0000	0b0000	0b000

Accessibility

MRS <Xt>, CSSELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CSSELR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = CSSELR_EL1;
```

MSR CSSELR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        CSSELR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    CSSELR_EL1 = X[t, 64];
```

A.2.1.42 CTR\_EL0, Cache Type Register

Provides information about the architecture of the caches.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx01	0100	0100	0100	10xx	xxxx	xxxx	0100
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-45: AARCH64\_CTR\_EL0 bit assignments

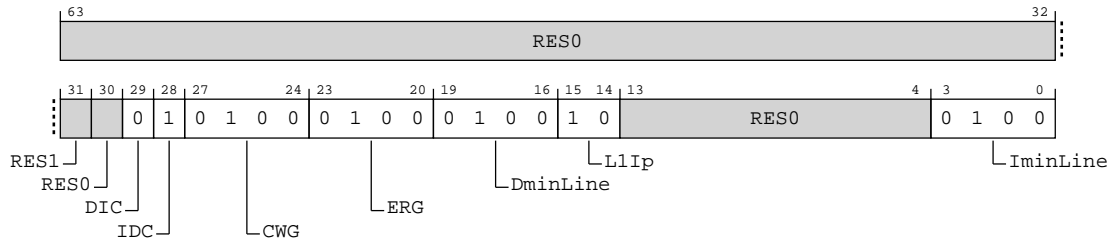


Table A-98: CTR\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	RES1	Reserved	RES1
[30]	RES0	Reserved	RES0
[29]	DIC	Instruction cache invalidation requirements for data to instruction coherence. <b>0b0</b> Instruction cache invalidation to the Point of Unification is required for data to instruction coherence.	0b0
[28]	IDC	Data cache clean requirements for instruction to data coherence. The meaning of this bit is: <b>0b1</b> Data cache clean to the Point of Unification is not required for instruction to data coherence.	0b1
[27:24]	CWG	Cache writeback granule. Log <sub>2</sub> of the number of words of the maximum size of memory that can be overwritten as a result of the eviction of a cache entry that has had a memory location in it modified. <b>0b0100</b> 64 bytes.	0b0100
[23:20]	ERG	Exclusives reservation granule. Log <sub>2</sub> of the number of words of the maximum size of the reservation granule that has been implemented for the Load-Exclusive and Store-Exclusive instructions. <b>0b0100</b> 64 bytes.	0b0100
[19:16]	DminLine	Log <sub>2</sub> of the number of words in the smallest cache line of all the data caches and unified caches that are controlled by the PE. <b>0b0100</b> 64 bytes.	0b0100
[15:14]	L1Ip	Level 1 instruction cache policy. Indicates the indexing and tagging policy for the L1 instruction cache. Possible values of this field are: <b>0b10</b> Virtual Index, Physical Tag (VIPT).	0b10
[13:4]	RES0	Reserved	RES0
[3:0]	IminLine	Log <sub>2</sub> of the number of words in the smallest cache line of all the instruction caches that are controlled by the PE. <b>0b0100</b> 64 bytes.	0b0100

Access

MRS <Xt>, CTR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b0000	0b0000	0b001

Accessibility

MRS <Xt>, CTR\_ELO

```
if PSTATE.EL == EL0 then
    if SCTLR_EL1.UCT == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CTR_ELO;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID2 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CTR_ELO;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CTR_ELO;
```

A.2.1.43 DCZID\_ELO, Data Cache Zero ID Register

Indicates the block size that is written with byte values of 0 by the DC ZVA (Data Cache Zero by Address) System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-46: AARCH64\_DCZID\_ELO bit assignments

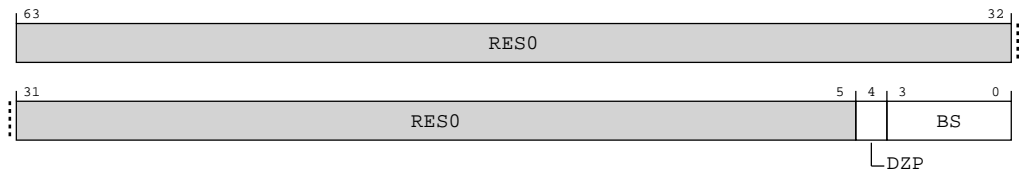


Table A-100: DCZID\_ELO bit descriptions

Bits	Name	Description	Reset
[63:5]	RES0	Reserved	RES0
[4]	DZP	Data Zero Prohibited. This field indicates whether use of DC ZVA instructions is permitted or prohibited.  0b0 Instructions are permitted.  0b1 Instructions are prohibited.  The value read from this field is governed by the access state and the values of the AArch64-HCR_EL2.TDZ and AArch64-SCTLR_EL1.DZE bits.	x
[3:0]	BS	Log <sub>2</sub> of the block size in words. The maximum size supported is 2KB, indicated by value 0b1001.	xxxx

Access

MRS <Xt>, DCZID\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b0000	0b0000	0b111

Accessibility

MRS <Xt>, DCZID\_ELO

```
if PSTATE.EL == EL0 then
    X[t, 64] = DCZID_EL0;
elsif PSTATE.EL == EL1 then
    X[t, 64] = DCZID_EL0;
elsif PSTATE.EL == EL2 then
    X[t, 64] = DCZID_EL0;
```



A.2.1.44 VPIDR\_EL2, Virtualization Processor ID Register

Holds the value of the Virtualization Processor ID. This is the value returned by EL1 reads of AArch64-MIDR\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

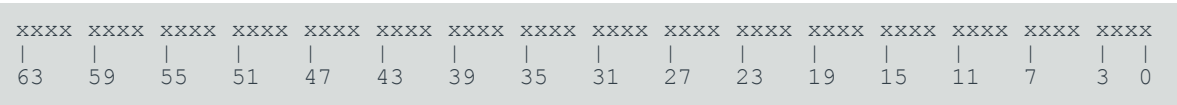
Functional group

Identification registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-47: AARCH64\_VPIDR\_EL2 bit assignments

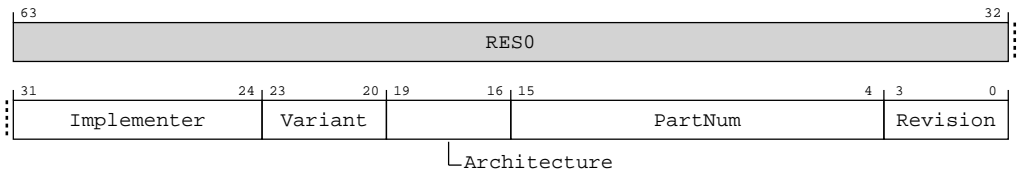


Table A-102: VPIDR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:24]	Implementer	<p>The Implementer code. This field must hold an implementer code that has been assigned by Arm. Assigned codes include the following:</p> <p><b>0b00000000</b> Reserved for software use.</p> <p><b>0b01000001</b> Arm Limited.</p> <p><b>0b01000010</b> Broadcom Corporation.</p> <p><b>0b01000011</b> Cavium Inc.</p> <p><b>0b01000100</b> Digital Equipment Corporation.</p> <p><b>0b01000110</b> Fujitsu Ltd.</p> <p><b>0b01001001</b> Infineon Technologies AG.</p> <p><b>0b01001101</b> Motorola or Freescale Semiconductor Inc.</p> <p><b>0b01001110</b> NVIDIA Corporation.</p> <p><b>0b01010000</b> Applied Micro Circuits Corporation.</p> <p><b>0b01010001</b> Qualcomm Inc.</p> <p><b>0b01010110</b> Marvell International Ltd.</p> <p><b>0b01101001</b> Intel Corporation.</p> <p><b>0b11000000</b> Ampere Computing.</p> <p>Arm can assign codes that are not published in this manual. All values not assigned by Arm are reserved and must not be used.</p>	8 {x}
[23:20]	Variant	An <b>IMPLEMENTATION DEFINED</b> variant number. Typically, this field is used to distinguish between different product variants, or major revisions of a product.	xxx

Bits	Name	Description	Reset
[19:16]	Architecture	<p>Architecture version. Defined values are:</p> <p><b>0b0001</b> Armv4.</p> <p><b>0b0010</b> Armv4T.</p> <p><b>0b0011</b> Armv5 (obsolete).</p> <p><b>0b0100</b> Armv5T.</p> <p><b>0b0101</b> Armv5TE.</p> <p><b>0b0110</b> Armv5TEJ.</p> <p><b>0b0111</b> Armv6.</p> <p><b>0b1111</b> Architectural features are individually identified in the ID_* registers.</p> <p>All other values are reserved.</p>	xxxx
[15:4]	PartNum	<p>An <b>IMPLEMENTATION DEFINED</b> primary part number for the device.</p> <p>On processors implemented by Arm, if the top four bits of the primary part number are 0x0 or 0x7, the variant and architecture are encoded differently.</p>	12{x}
[3:0]	Revision	An <b>IMPLEMENTATION DEFINED</b> revision number for the device.	xxxx

### Access

MRS <Xt>, VPIDR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0000	0b0000	0b000

MSR VPIDR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0000	0b0000	0b000

MRS <Xt>, MIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b000

## Accessibility

MRS <Xt>, VPIDR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VPIDR_EL2;

```

MSR VPIDR\_EL2, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VPIDR_EL2 = X[t, 64];

```

MRS <Xt>, MIDR\_EL1

```

if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    X[t, 64] = VPIDR_EL2;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MIDR_EL1;

```

### A.2.1.45 VMPIDR\_EL2, Virtualization Multiprocessor ID Register

Holds the value of the Virtualization Multiprocessor ID. This is the value returned by EL1 reads of AArch64-MPIDR\_EL1.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Identification registers

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx

63 59 55 51 47 43 39 35 31 27 23 19 15 11 7 3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-48: AARCH64\_VMPIDR\_EL2 bit assignments

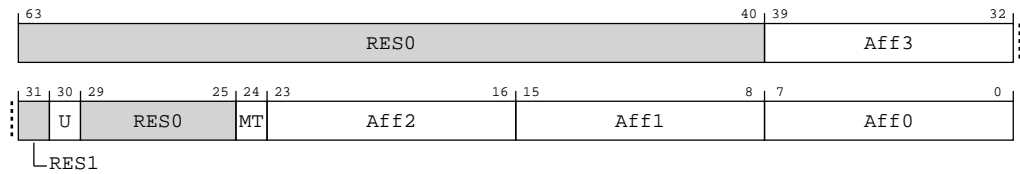


Table A-106: VMPIDR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	Aff3	Affinity level 3. See the description of VMPIDR_EL2.Aff0 for more information.	8 {x}
[31]	RES1	Reserved	RES1
[30]	U	Indicates a Uniprocessor system, as distinct from PE 0 in a multiprocessor system.  <b>0b0</b> Processor is part of a multiprocessor system.  <b>0b1</b> Processor is part of a uniprocessor system.	x
[29:25]	RES0	Reserved	RES0
[24]	MT	Indicates whether the lowest level of affinity consists of logical PEs that are implemented using a multithreading type approach. See the description of VMPIDR_EL2.Aff0 for more information about affinity levels.  <b>0b0</b> Performance of PEs at the lowest affinity level is largely independent.  <b>0b1</b> Performance of PEs at the lowest affinity level is very interdependent.	x
[23:16]	Aff2	Affinity level 2. See the description of VMPIDR_EL2.Aff0 for more information.	8 {x}
[15:8]	Aff1	Affinity level 1. See the description of VMPIDR_EL2.Aff0 for more information.	8 {x}
[7:0]	Aff0	Affinity level 0. This is the affinity level that is most significant for determining PE behavior. Higher affinity levels are increasingly less significant in determining PE behavior.  The assigned value of the AArch64-MPIDR_EL1.{Aff3, Aff2, Aff1, Aff0} set of fields of each PE must be unique within the system as a whole.	8 {x}

## Access

MRS <Xt>, VMPIDR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0000	0b0000	0b101

MSR VMPIDR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0000	0b0000	0b101

MRS <Xt>, MPIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b101

Accessibility

MRS <Xt>, VMPIDR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VMPIDR_EL2;
```

MSR VMPIDR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VMPIDR_EL2 = X[t, 64];
```

MRS <Xt>, MPIDR\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    X[t, 64] = VMPIDR_EL2;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MPIDR_EL1;
```

A.2.2 AArch64 Generic System control register description

This section includes the register descriptions for all Generic System control registers in the Cortex®-R82AE processor.

A.2.2.1 MPUIR\_EL1, MPU Type Register (EL1)

Identifies the number of regions supported by the EL1 MPU.

Configurations

This register is available in all configurations.

Attributes

Width

64

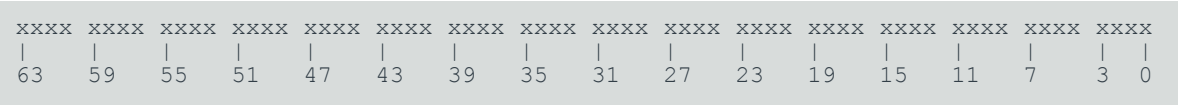
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-49: AARCH64\_MPUIR\_EL1 bit assignments

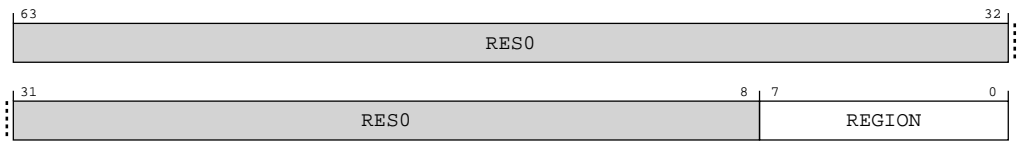


Table A-110: MPUIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	REGION	The number of EL1 MPU regions supported.	8 {x}

Access

MRS <Xt>, MPUIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0000	0b100

Accessibility

MRS <Xt>, MPUIR\_EL1

```
if PSTATE.EL == EL0 then
  if HCR_EL2.TGE == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
  if HCR_EL2.TID1 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  elseif VTCR_EL2.MSA == '1' then
    UNDEFINED;
  else
    X[t, 64] = MPUIR_EL1;
elseif PSTATE.EL == EL2 then
  X[t, 64] = MPUIR_EL1;
```

A.2.2.2 SCTRL\_EL1, System Control Register (EL1)

Provides top level control of the system, including its memory system, at EL1 and EL0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.



## Bit descriptions

Figure A-50: AARCH64\_SCTLR\_EL1 bit assignments

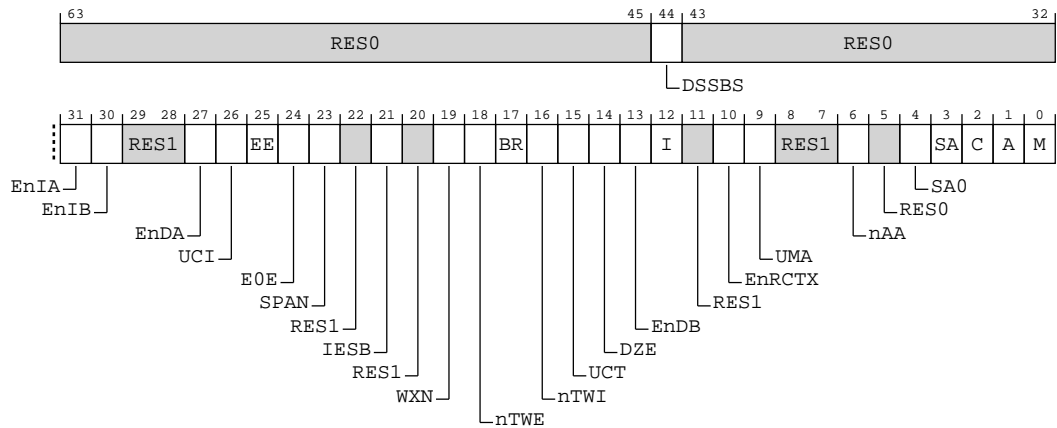


Table A-112: SCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:45]	RES0	Reserved	RES0
[44]	DSSBS	Default PSTATE.SSBS value on Exception Entry.  <b>0b0</b> PSTATE.SSBS is set to 0 on an exception to EL1.  <b>0b1</b> PSTATE.SSBS is set to 1 on an exception to EL1.	x
[43:32]	RES0	Reserved	RES0
[31]	EnIA	Controls enabling of pointer authentication of instruction addresses, using the APIAKey_EL1 key, in the EL1&O translation regime.  <b>0b0</b> Pointer authentication of instruction addresses, using the APIAKey_EL1 key, is not enabled.  <b>0b1</b> Pointer authentication of instruction addresses, using the APIAKey_EL1 key, is enabled.  <b>Note:</b> This field controls the behavior of the AddPACIA and AuthIA pseudocode functions. Specifically, when the field is 1, AddPACIA returns a copy of a pointer to which a pointer authentication code has been added, and AuthIA returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b> .	x

Bits	Name	Description	Reset
[30]	EnIB	<p>Controls enabling of pointer authentication of instruction addresses, using the APIBKey_EL1 key, in the EL1&amp;O translation regime.</p> <p><b>0b0</b></p> <p>Pointer authentication of instruction addresses, using the APIBKey_EL1 key, is not enabled.</p> <p><b>0b1</b></p> <p>Pointer authentication of instruction addresses, using the APIBKey_EL1 key, is enabled.</p> <p><b>Note:</b></p> <p>This field controls the behavior of the AddPACIB and AuthIB pseudocode functions. Specifically, when the field is 1, AddPACIB returns a copy of a pointer to which a pointer authentication code has been added, and AuthIB returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b>.</p>	x
[29:28]	<b>RES1</b>	Reserved	<b>RES1</b>
[27]	EnDA	<p>Controls enabling of pointer authentication of instruction addresses, using the APDAKey_EL1 key, in the EL1&amp;O translation regime.</p> <p><b>0b0</b></p> <p>Pointer authentication of data addresses, using the APDAKey_EL1 key, is not enabled.</p> <p><b>0b1</b></p> <p>Pointer authentication of data addresses, using the APDAKey_EL1 key, is enabled.</p> <p><b>Note:</b></p> <p>This field controls the behavior of the AddPACDA and AuthDA pseudocode functions. Specifically, when the field is 1, AddPACDA returns a copy of a pointer to which a pointer authentication code has been added, and AuthDA returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b>.</p>	x
[26]	UCI	<p>Traps ELO execution of cache maintenance instructions, to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from AArch64 state only, reported using an ESR_ELx.EC value of 0x18.</p> <p>This applies to DC CVAU, DC CIVAC, DC CVAC, DC CVAP, and IC IVAU.</p> <p>If FEAT_DPB2 is implemented, this trap also applies to DC CVADP.</p> <p><b>0b0</b></p> <p>Execution of the specified instructions at ELO using AArch64 is trapped.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[25]	EE	<p>Endianness of data accesses at EL1, and stage 1 translation table walks in the EL1&amp;O translation regime.</p> <p><b>0b0</b></p> <p>Explicit data accesses at EL1, and stage 1 translation table walks in the EL1&amp;O translation regime are little-endian.</p> <p><b>0b1</b></p> <p>Explicit data accesses at EL1, and stage 1 translation table walks in the EL1&amp;O translation regime are big-endian.</p> <p>The EE bit is permitted to be cached in a TLB.</p>	x

Bits	Name	Description	Reset
[24]	EOE	<p>Endianness of data accesses at EL0.</p> <p><b>0b0</b> Explicit data accesses at EL0 are little-endian.</p> <p><b>0b1</b> Explicit data accesses at EL0 are big-endian.</p> <p>This bit has no effect on the endianness of LDTR, LDTRH, LDTRSH, LDTRSW, STTR, and STTRH instructions executed at EL1.</p>	x
[23]	SPAN	<p>Set Privileged Access Never, on taking an exception to EL1.</p> <p><b>0b0</b> PSTATE.PAN is set to 1 on taking an exception to EL1.</p> <p><b>0b1</b> The value of PSTATE.PAN is left unchanged on taking an exception to EL1.</p>	x
[22]	RES1	Reserved	RES1
[21]	IESB	<p>Implicit Error Synchronization event enable. Possible values are:</p> <p><b>0b0</b> Disabled.</p> <p><b>0b1</b> An implicit error synchronization event is added:</p> <ul style="list-style-type: none"> <li>At each exception taken to EL1.</li> <li>Before the operational pseudocode of each ERET instruction executed at EL1.</li> </ul> <p>When the PE is in Debug state, this field has no effect.</p>	x
[20]	RES1	Reserved	RES1
[19]	WXN	<p>Write permission implies XN (Execute-never). For the EL1&amp;O translation regime, this bit can force all memory regions that are writable to be treated as XN.</p> <p><b>0b0</b> This control has no effect on memory access permissions.</p> <p><b>0b1</b> Any region that is writable in the EL1&amp;O translation regime is forced to XN for accesses from software executing at EL1 or EL0.</p> <p>This bit applies only when SCTLR_EL1.M bit is set.</p> <p>The WXN bit is permitted to be cached in a TLB.</p>	x

Bits	Name	Description	Reset
[18]	nTWE	<p>Traps ELO execution of WFE instructions to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from both Execution states, reported using an ESR_ELx.EC value of 0x01.</p> <p><b>0b0</b></p> <p>Any attempt to execute a WFE instruction at ELO is trapped, if the instruction would otherwise have caused the PE to enter a low-power state.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>Note:</b></p> <p>Since a WFE or WFI can complete at any time, even without a Wakeup event, the traps on WFE or WFI are not guaranteed to be taken, even if the WFE or WFI is executed when there is no Wakeup event. The only guarantee is that if the instruction does not complete in finite time in the absence of a Wakeup event, the trap will be taken.</p>	x
[17]	BR	<p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>Background region enable for EL1 MPU memory regions.</p> <p><b>0b0</b></p> <p>Background region disabled for stage 1 EL1&amp;O translation regime.</p> <p><b>0b1</b></p> <p>Background region enabled for stage 1 EL1&amp;O translation regime.</p> <p>If the value of AArch64-HCR_EL2.{DC, TGE} is not {0, 0} then PE behaves as if the value of the AArch64-SCTLR_EL1.BR field is 0 for all purposes other than returning the value of a direct read of the field.</p> <p>If EL1 MPU is enabled, then ELO access that does not match an EL1 MPU region always results in a Translation fault.</p> <p><b>Otherwise</b></p> <p>RES0</p>	'0'
[16]	nTWI	<p>Traps ELO execution of WFI instructions to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from both Execution states, reported using an ESR_ELx.EC value of 0x01.</p> <p><b>0b0</b></p> <p>Any attempt to execute a WFI instruction at ELO is trapped, if the instruction would otherwise have caused the PE to enter a low-power state.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>Note:</b></p> <p>Since a WFE or WFI can complete at any time, even without a Wakeup event, the traps on WFE or WFI are not guaranteed to be taken, even if the WFE or WFI is executed when there is no Wakeup event. The only guarantee is that if the instruction does not complete in finite time in the absence of a Wakeup event, the trap will be taken.</p>	x

Bits	Name	Description	Reset
[15]	UCT	<p>Traps ELO accesses to the AArch64-CTR_ELO to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from AArch64 state only, reported using an ESR_ELx.EC value of 0x18.</p> <p><b>0b0</b></p> <p>Accesses to the AArch64-CTR_ELO from EL0 using AArch64 are trapped.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[14]	DZE	<p>Traps ELO execution of DC ZVA instructions to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from AArch64 state only, reported using an ESR_ELx.EC value of 0x18.</p> <p><b>0b0</b></p> <p>Any attempt to execute an instruction that this trap applies to at EL0 using AArch64 is trapped.</p> <p>Reading AArch64-DCZID_ELO.DZP from EL0 returns 1, indicating that the instructions this trap applies to are not supported.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[13]	EnDB	<p>Controls enabling of pointer authentication of instruction addresses, using the APDBKey_EL1 key, in the EL1&amp;0 translation regime.</p> <p><b>0b0</b></p> <p>Pointer authentication of data addresses, using the APDBKey_EL1 key, is not enabled.</p> <p><b>0b1</b></p> <p>Pointer authentication of data addresses, using the APDBKey_EL1 key, is enabled.</p> <p><b>Note:</b></p> <p>This field controls the behavior of the AddPACDB and AuthDB pseudocode functions. Specifically, when the field is 1, AddPACDB returns a copy of a pointer to which a pointer authentication code has been added, and AuthDB returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b>.</p>	x

Bits	Name	Description	Reset
[12]	I	<p>Stage 1 instruction access Cacheability control, for accesses at ELO and EL1:</p> <p><b>0b0</b></p> <p>All instruction access to Stage 1 Normal memory from ELO and EL1 are Stage 1 Non-cacheable.</p> <p>If stage 1 EL1&amp;0 translation is in VMSAv8-64 context and the value of SCTLR_EL1.M is 0, then instruction accesses from stage 1 are to Normal, Outer Shareable, Inner Non-cacheable, Outer Non-cacheable memory.</p> <p>If stage 1 EL1&amp;0 translation is in PMSAv8-64 context and the value of SCTLR_EL1.{BR, M} = {0, 0}, then instruction accesses from stage 1 are to Normal, Outer Shareable, Inner Non-cacheable, Outer Non-cacheable memory.</p> <p><b>0b1</b></p> <p>This control has no effect on the Stage 1 Cacheability of instruction access to Stage 1 Normal memory from ELO and EL1.</p> <p>If stage 1 EL1&amp;0 translation is in VMSAv8-64 context and the value of SCTLR_EL1.M is 0, then instruction accesses from stage 1 are to Normal, Outer Shareable, Inner Write-Through, Outer Write-Through memory.</p> <p>If stage 1 EL1&amp;0 translation is in PMSAv8-64 context, and the value of SCTLR_EL1.{BR, M} = {0, 0}, then instruction accesses from stage 1 are to Normal, Outer Shareable, Inner Write-Through, Outer Write-Through memory.</p> <p>When the value of the AArch64-HCR_EL2.DC bit is 1, then instruction access to Normal memory from ELO and EL1 are Cacheable regardless of the value of the SCTLR_EL1.I bit.</p>	x
[11]	RES1	Reserved	RES1
[10]	EnRCTX	<p>Enable ELO access to the following System instructions:</p> <ul style="list-style-type: none"> <li>CFP RCTX, DVP RCTX and CPP RCTX instructions.</li> </ul> <p><b>0b0</b></p> <p>ELO access to these instructions is disabled, and these instructions are trapped to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1.</p> <p><b>0b1</b></p> <p>ELO access to these instructions is enabled.</p>	x
[9]	UMA	<p>User Mask Access. Traps ELO execution of MSR and MRS instructions that access the PSTATE.{D, A, I, F} masks to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from AArch64 state only, reported using an ESR_ELx.EC value of 0x18.</p> <p><b>0b0</b></p> <p>Any attempt at ELO using AArch64 to execute an MRS, MSR(<i>register</i>), or MSR(<i>immediate</i>) instruction that accesses the AArch64-DAIF is trapped.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[8:7]	RES1	Reserved	RES1

Bits	Name	Description	Reset
[6]	nAA	<p>Non-aligned access. This bit controls generation of Alignment faults at EL1 and EL0 under certain conditions.</p> <p>The following instructions generate an Alignment fault if all bytes being accessed are not within a single 16-byte quantity, aligned to 16 bytes for access:</p> <ul style="list-style-type: none"> <li>LDAPR, LDAPRH, LDAPUR, LDAPURH, LDAPURSH, LDAPURSW, LDAR, LDARH, LDLAR, LDLARH.</li> <li>STLLR, STLLRH, STLR, STLRH, STLUR, and STLURH.</li> </ul> <p><b>0b0</b></p> <p>Unaligned accesses by the specified instructions generate an Alignment fault.</p> <p><b>0b1</b></p> <p>This control does not generate Alignment faults.</p>	x
[5]	RES0	Reserved	RES0
[4]	SA0	SP Alignment check enable for EL0. When set to 1, if a load or store instruction executed at EL0 uses the SP as the base address and the SP is not aligned to a 16-byte boundary, then an SP alignment fault exception is generated. For more information, see <i>SP alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x
[3]	SA	SP Alignment check enable. When set to 1, if a load or store instruction executed at EL1 uses the SP as the base address and the SP is not aligned to a 16-byte boundary, then an SP alignment fault exception is generated. For more information, see <i>SP alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x
[2]	C	<p>Stage 1 Cacheability control, for data accesses.</p> <p><b>0b0</b></p> <p>All data access to Stage 1 Normal memory from EL0 and EL1, and all Normal memory accesses from unified cache to the EL1&amp;0 Stage 1 translation tables, are treated as Stage 1 Non-cacheable.</p> <p><b>0b1</b></p> <p>This control has no effect on the Stage 1 Cacheability of:</p> <ul style="list-style-type: none"> <li>Data access to Normal memory from EL0 and EL1.</li> <li>Normal memory accesses to the EL1&amp;0 Stage 1 translation tables.</li> </ul> <p>When the Effective value of the HCR_EL2.DC bit in the current Security state is 1, the PE ignores SCTLR_EL1.C. This means that EL0 and EL1 data accesses to Normal memory are Cacheable.</p>	x
[1]	A	<p>Alignment check enable. This is the enable bit for Alignment fault checking at EL1 and EL0.</p> <p><b>0b0</b></p> <p>Alignment fault checking is disabled when executing at EL1 or EL0.</p> <p>Alignment checks on some instructions are not disabled by this control. For more information, see <i>Alignment of data accesses</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b1</b></p> <p>Alignment fault checking is enabled when executing at EL1 or EL0.</p> <p>All instructions that load or store one or more registers have an alignment check that the address being accessed is aligned to the size of the data element(s) being accessed. If this check fails it causes an Alignment fault, which is taken as a Data Abort exception.</p>	x

Bits	Name	Description	Reset
[0]	M	<p>MMU or MPU enable for EL1&amp;O stage 1 address translation.</p> <p>This is the enable bit for:</p> <ul style="list-style-type: none"> <li>MPU, if stage 1 EL1&amp;O translation is in PMSAv8-64 context.</li> <li>MMU, if stage 1 EL1&amp;O translation is in VMSAv8-64 context.</li> </ul> <p><b>0b0</b></p> <p>EL1 MPU(PMSAv8-64) or MMU(VMSAv8-64) disabled</p> <p>See the SCTLR_EL1.I field for the behavior of instruction accesses to Normal memory.</p> <p><b>0b1</b></p> <p>EL1 MPU(PMSAv8-64) or MMU(VMSAv8-64) enabled</p> <p>If the Effective value of HCR_EL2.{DC, TGE} in the current Security state is not {0, 0} then the PE behaves as if the value of the SCTLR_EL1.M field is 0 for all purposes other than returning the value of a direct read of the field.</p>	x

## Access

MRS <Xt>, SCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b000

MSR SCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b000

## Accessibility

MRS <Xt>, SCTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = SCTLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = SCTLR_EL1;

```

MSR SCTLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SCTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then

```



```
SCTLR_EL1 = X[t, 64];
```

A.2.2.3 ACTLR\_EL1, Auxiliary Control Register (EL1)

Provides **IMPLEMENTATION DEFINED** configuration and control options for execution at EL1 and EL0.

Configurations

This register is available in all configurations.

Attributes

Width

64

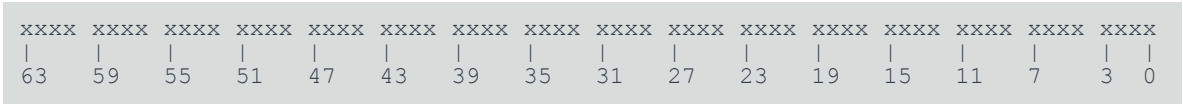
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-51: AARCH64\_ACTLR\_EL1 bit assignments

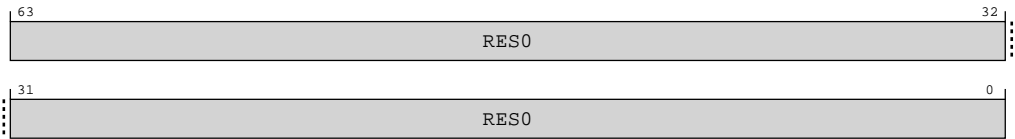


Table A-115: ACTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ACTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b001

MSR ACTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b001

Accessibility

MRS <Xt>, ACTLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TACR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ACTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ACTLR_EL1;
```

MSR ACTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TACR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ACTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ACTLR_EL1 = X[t, 64];
```

A.2.2.4 CPACR\_EL1, Architectural Feature Access Control Register

Controls access to trace,  
and Advanced SIMD and floating-point functionality.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-52: AARCH64\_CPACR\_EL1 bit assignments

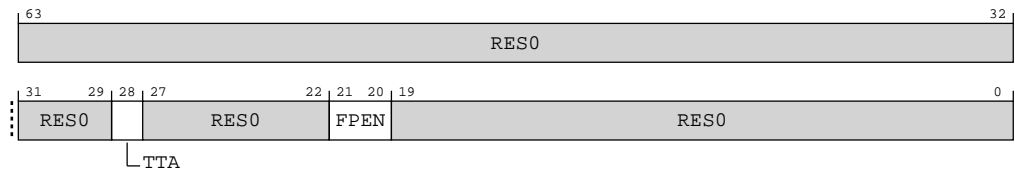


Table A-118: CPACR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:29]	RES0	Reserved	RES0
[28]	TTA	<p>Traps EL0 and EL1 System register accesses to all implemented trace registers from both Execution states to EL1, or to EL2 when it is implemented and enabled in the current Security state and AArch64-HCR_EL2.TGE is 1, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to trace registers are trapped, reported using ESR_ELx.EC value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>This control causes EL0 and EL1 System register accesses to all implemented trace registers to be trapped.</p> <ul style="list-style-type: none"> <li>The ETMv4 architecture does not permit EL0 to access the trace registers. If the trace unit implements FEAT_ETMv4, EL0 accesses to the trace registers are UNDEFINED, and any resulting exception is higher priority than an exception that would be generated because the value of AArch64-CPACR_EL1.TTA is 1.</li> <li>The Armv8-A architecture does not provide traps on trace register accesses through the optional memory-mapped interface.</li> </ul> <p>System register accesses to the trace registers can have side-effects. When a System register access is trapped, any side-effects that are normally associated with the access do not occur before the exception is taken.</p> <p>If System register access to the trace functionality is not implemented, this bit is <b>RES0</b>.</p>	x
[27:22]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[21:20]	FPEN	Traps execution at EL1 and EL0 of instructions that access the Advanced SIMD and floating-point registers from both Execution states to EL1, reported using ESR_ELx.EC value 0x07, or to EL2 reported using ESR_ELx.EC value 0x00 when EL2 is implemented and enabled in the current Security state and AArch64-HCR_EL2.TGE is 1, as follows: <ul style="list-style-type: none"><li>In AArch64 state, accesses to AArch64-FPCR, AArch64-FPSR, any of the SIMD and floating-point registers V0-V31, including their views as D0-D31 registers or S0-31 registers.</li></ul> <p><b>0b00</b></p> <p>This control causes execution of these instructions at EL1 and EL0 to be trapped.</p> <p><b>0b01</b></p> <p>This control causes execution of these instructions at EL0 to be trapped, but does not cause execution of any instructions at EL1 to be trapped.</p> <p><b>0b10</b></p> <p>This control causes execution of these instructions at EL1 and EL0 to be trapped.</p> <p><b>0b11</b></p> <p>This control does not cause execution of any instructions to be trapped.</p>	xx
[19:0]	RES0	Reserved	RES0

Access

MRS <Xt>, CPACR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b010

MSR CPACR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0000	0b010

Accessibility

MRS <Xt>, CPACR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPTR_EL2.TCPAC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CPACR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CPACR_EL1;
```

MSR CPACR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPTR_EL2.TCPAC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

```
CPACR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    CPACR_EL1 = X[t, 64];
```

A.2.2.5 TTBR0\_EL1, Translation Table Base Register 0 (EL1)

Holds the base address of the translation table for the initial lookup for stage 1 of the translation of an address from the lower VA range in the EL1&O translation regime, and other information for this translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0

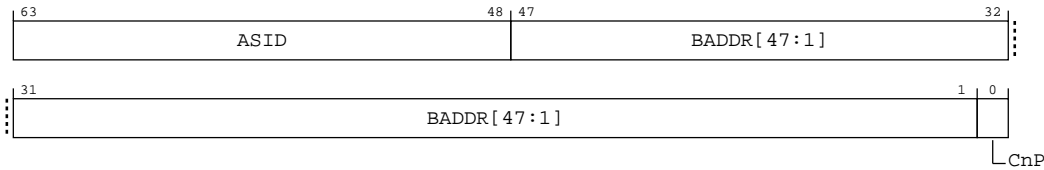


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-53: AARCH64\_TTBR0\_EL1 bit assignments



**Table A-121: TTBR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	ASID	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b> An ASID for the translation table base address. The AArch64-TCR_EL1.A1 field selects either TTBR0_EL1.ASID or TTBR1_EL1.ASID.</p> <p><b>When AArch64-VTCR_EL2.MSA == '0'</b> An ASID for addresses defined by the current EL1 MPU configuration.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[47:1]	BADDR[47:1]	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b> Translation table base address:</p> <ul style="list-style-type: none"> <li>Bits A[47:x] of the stage 1 translation table base address bits are in register bits[47:x]. - Bits A[(x-1):0] of the stage 1 translation table base address are zero.</li> </ul> <p>Address bit x is the minimum address bit required to align the translation table to the size of the table. The smallest permitted value of x is 6. The AArch64 Virtual Memory System Architecture chapter describes how x is calculated based on the value of AArch64-TCR_EL1.TOSZ, the translation stage, and the translation granule size.</p> <p><b>Note:</b> A translation table is required to be aligned to the size of the table. If a table contains fewer than eight entries, it must be aligned on a 64 byte address boundary.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[0]	CnP	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Common not Private. This bit indicates whether each entry that is pointed to by TTBR0_EL1 is a member of a common set that can be used by every PE in the Inner Shareable domain for which the value of TTBR0_EL1.CnP is 1.</p> <p><b>0b0</b></p> <p>The translation table entries pointed to by TTBR0_EL1, for the current translation regime and ASID, are permitted to differ from corresponding entries for TTBR0_EL1 for other PEs in the Inner Shareable domain. This is not affected by:</p> <ul style="list-style-type: none"> <li>• The value of TTBR0_EL1.CnP on those other PEs.</li> <li>• The value of the current ASID.</li> <li>• If EL2 is implemented and enabled in the current Security state, the value of the current VMID.</li> </ul> <p><b>0b1</b></p> <p>The translation table entries pointed to by TTBR0_EL1 are the same as the translation table entries for every other PE in the Inner Shareable domain for which the value of TTBR0_EL1.CnP is 1 and all of the following apply:</p> <ul style="list-style-type: none"> <li>• The translation table entries are pointed to by TTBR0_EL1.</li> <li>• The translation tables relate to the same translation regime.</li> <li>• The ASID is the same as the current ASID.</li> <li>• If EL2 is implemented and enabled in the current Security state, the value of the current VMID.</li> </ul> <p>This bit is permitted to be cached in a TLB.</p> <p>When a TLB combines entries from stage 1 translation and stage 2 translation into a single entry, that entry can only be shared between different PEs if the value of the CnP bit is 1 for both stage 1 and stage 2.</p> <p><b>Note:</b></p> <p>If the value of the TTBR0_EL1.CnP bit is 1 on multiple PEs in the same Inner Shareable domain and those TTBR0_EL1s do not point to the same translation table entries when the other conditions specified for the case when the value of CnP is 1 apply, then the results of translations are <b>CONSTRAINED UNPREDICTABLE</b>, see <b>CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values</b> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>RES0</p> <p><b>Otherwise</b></p> <p>RES0</p>	x

## Access

MRS <Xt>, TTBR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b000

MSR TTBR0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b000

Accessibility

MRS <Xt>, TTBR0\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TTBR0_EL1<63:0>;
elsif PSTATE.EL == EL2 then
    X[t, 64] = TTBR0_EL1<63:0>;
```

MSR TTBR0\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TTBR0_EL1<63:0> = X[t, 64];
elsif PSTATE.EL == EL2 then
    TTBR0_EL1<63:0> = X[t, 64];
```

A.2.2.6 TTBR1\_EL1, Translation Table Base Register 1 (EL1)

Holds the base address of the translation table for the initial lookup for stage 1 of the translation of an address from the higher VA range in the EL1&O stage 1 translation regime, and other information for this translation regime.

Configurations

In a PMSAv8-64 only implementation, this register is UNDEFINED.

This register is present only when ArchHasVMSAExtension(). Otherwise, direct accesses to TTBR1\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

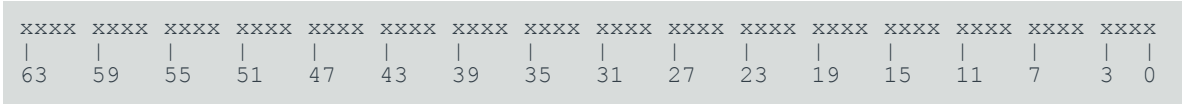
Generic System Control

Access type

See bit descriptions



Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-54: AArch64\_TTBR1\_EL1 bit assignments

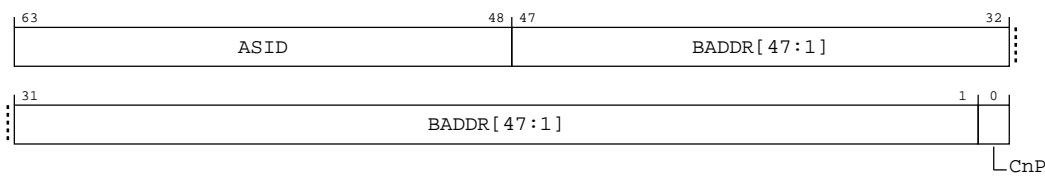


Table A-124: TTBR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	<b>When AArch64-VTCR_EL2.MSA == '1'</b> An ASID for the translation table base address. The AArch64-TCR_EL1.A1 field selects either TTBR0_EL1.ASID or TTBR1_EL1.ASID. If the implementation has only 8 bits of ASID, then the upper 8 bits of this field are <b>RES0</b> .  <b>Otherwise</b> RES0	xxxx
[47:1]	BADDR[47:1]	<b>When AArch64-VTCR_EL2.MSA == '1'</b> Translation table base address: <ul style="list-style-type: none"><li>Bits A[47:x] of the stage 1 translation table base address bits are in register bits[47:x]. - Bits A[(x-1):0] of the stage 1 translation table base address are zero.</li></ul> Address bit x is the minimum address bit required to align the translation table to the size of the table. The smallest permitted value of x is 6. The AArch64 Virtual Memory System Architecture chapter describes how x is calculated based on the value of AArch64-TCR_EL1.T1SZ, the translation stage, and the translation granule size. <b>Note:</b> A translation table is required to be aligned to the size of the table. If a table contains fewer than eight entries, it must be aligned on a 64 byte address boundary.  <b>Otherwise</b> RES0	xxxx

Bits	Name	Description	Reset
[0]	CnP	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Common not Private. This bit indicates whether each entry that is pointed to by TBR1_EL1 is a member of a common set that can be used by every PE in the Inner Shareable domain for which the value of TTBR1_EL1.CnP is 1.</p> <p><b>0b0</b></p> <p>The translation table entries pointed to by TTBR1_EL1, for the current translation regime and ASID, are permitted to differ from corresponding entries for TTBR1_EL1 for other PEs in the Inner Shareable domain. This is not affected by:</p> <ul style="list-style-type: none"> <li>• The value of TTBR1_EL1.CnP on those other PEs.</li> <li>• The value of the current ASID.</li> <li>• If EL2 is implemented and enabled in the current Security state, the value of the current VMID.</li> </ul> <p><b>0b1</b></p> <p>The translation table entries pointed to by TTBR1_EL1 are the same as the translation table entries for every other PE in the Inner Shareable domain for which the value of TTBR1_EL1.CnP is 1 and all of the following apply:</p> <ul style="list-style-type: none"> <li>• The translation table entries are pointed to by TTBR1_EL1.</li> <li>• The translation tables relate to the same translation regime.</li> <li>• The ASID is the same as the current ASID.</li> <li>• If EL2 is implemented and enabled in the current Security state, the value of the current VMID.</li> </ul> <p>This bit is permitted to be cached in a TLB.</p> <p>When a TLB combines entries from stage 1 translation and stage 2 translation into a single entry, that entry can only be shared between different PEs if the value of the CnP bit is 1 for both stage 1 and stage 2.</p> <p><b>Note:</b></p> <p>If the value of the TTBR1_EL1.CnP bit is 1 on multiple PEs in the same Inner Shareable domain and those TTBR1_EL1s do not point to the same translation table entries when the other conditions specified for the case when the value of CnP is 1 apply, then the results of translations are <b>CONSTRAINED UNPREDICTABLE</b>, see <b>CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values</b> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx

## Access

MRS <Xt>, TTBR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b001

MSR TTBR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b001

## Accessibility

MRS <Xt>, TTBR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ID_AA64MMFR0_EL1.MSA_frac == '0001' then
        UNDEFINED;
    elsif HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif VTCR_EL2.MSA == '0' then
        UNDEFINED;
    else
        X[t, 64] = TTBR1_EL1<63:0>;
elsif PSTATE.EL == EL2 then
    if ID_AA64MMFR0_EL1.MSA_frac == '0001' then
        UNDEFINED;
    else
        X[t, 64] = TTBR1_EL1<63:0>;

```

MSR TTBR1\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ID_AA64MMFR0_EL1.MSA_frac == '0001' then
        UNDEFINED;
    elsif HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif VTCR_EL2.MSA == '0' then
        UNDEFINED;
    else
        TTBR1_EL1<63:0> = X[t, 64];
elsif PSTATE.EL == EL2 then
    if ID_AA64MMFR0_EL1.MSA_frac == '0001' then
        UNDEFINED;
    else
        TTBR1_EL1<63:0> = X[t, 64];

```

### A.2.2.7 TCR\_EL1, Translation Control Register (EL1)

The control register for stage 1 of the EL1&0 translation regime.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic System Control

##### Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

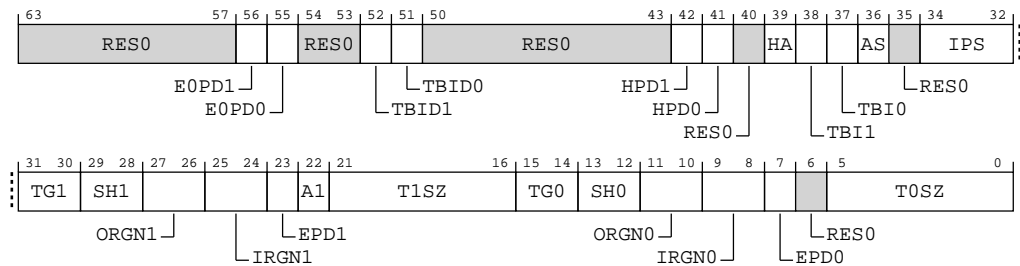


Where the reset reads xxxx, see individual bits.

## Bit descriptions

Any of the bits in TCR\_EL1, other than the A1 bit and the EPDx bits when they have the value 1, are permitted to be cached in a TLB.

**Figure A-55: AARCH64\_TCR\_EL1 bit assignments**



**Table A-127: TCR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:57]	RES0	Reserved	RES0
[56]	EOPD1	<b>When AArch64-VTCR_EL2.MSA == '1'</b> Faulting control for Unprivileged access to any address translated by AArch64-TTBR1_EL1. <b>0b0</b> Unprivileged access to any address translated by AArch64-TTBR1_EL1 will not generate a fault by this mechanism. <b>0b1</b> Unprivileged access to any address translated by AArch64-TTBR1_EL1 will generate a level 0 Translation fault. Level 0 Translation faults generated as a result of this field are not counted as TLB misses for performance monitoring. The fault should take the same time to generate, whether the address is present in the TLB or not, to mitigate attacks that use fault timing. <b>Otherwise</b> RES0	xxxx

Bits	Name	Description	Reset
[55]	EOPDO	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Faulting control for Unprivileged access to any address translated by AArch64-TTBR0_EL1.</p> <p><b>0b0</b></p> <p>Unprivileged access to any address translated by AArch64-TTBR0_EL1 will not generate a fault by this mechanism.</p> <p><b>0b1</b></p> <p>Unprivileged access to any address translated by AArch64-TTBR0_EL1 will generate a level 0 Translation fault.</p> <p>Level 0 Translation faults generated as a result of this field are not counted as TLB misses for performance monitoring. The fault should take the same time to generate, whether the address is present in the TLB or not, to mitigate attacks that use fault timing.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx
[54:53]	RES0	Reserved	RES0
[52]	TBID1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Controls the use of the top byte of instruction addresses for address matching.</p> <p>For the purpose of this field, all cache maintenance and address translation instructions that perform address translation are treated as data accesses.</p> <p>For more information, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b0</b></p> <p>TCR_EL1.TBI1 applies to Instruction and Data accesses.</p> <p><b>0b1</b></p> <p>TCR_EL1.TBI1 applies to Data accesses only.</p> <p>This affects addresses where the address would be translated by tables pointed to by AArch64-TTBR1_EL1.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx

Bits	Name	Description	Reset
[51]	TBID0	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Controls the use of the top byte of instruction addresses for address matching. For the purpose of this field, all cache maintenance and address translation instructions that perform address translation are treated as data accesses. For more information, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b0</b> TCR_EL1.TBID0 applies to Instruction and Data accesses.</p> <p><b>0b1</b> TCR_EL1.TBID0 applies to Data accesses only.</p> <p>This affects addresses where the address would be translated by tables pointed to by AArch64-TTBR0_EL1.</p> <p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>Controls the use of the top byte of instruction addresses for address matching. For the purpose of this field, all cache maintenance and address translation instructions that perform address translation are treated as data accesses. For more information, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b0</b> TCR_EL1.TBID0 applies to Instruction and Data accesses.</p> <p><b>0b1</b> TCR_EL1.TBID0 applies to Data accesses only.</p> <p>This affects addresses where the address would be translated by EL1 MPU.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[50:43]	RES0	Reserved	RES0
[42]	HPD1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Hierarchical Permission Disables. This affects the hierarchical control bits, APTTable, PXNTable, and UXNTable, except NSTable, in the translation tables pointed to by AArch64-TTBR1_EL1.</p> <p><b>0b0</b> Hierarchical permissions are enabled.</p> <p><b>0b1</b> Hierarchical permissions are disabled.</p> <p>When disabled, the permissions are treated as if the bits are zero.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[41]	HPD0	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Hierarchical Permission Disables. This affects the hierarchical control bits, APTable, PXNTable, and UXNTable, except NSTable, in the translation tables pointed to by AArch64-TTBR0_EL1.</p> <p><b>0b0</b></p> <p>Hierarchical permissions are enabled.</p> <p><b>0b1</b></p> <p>Hierarchical permissions are disabled.</p> <p>When disabled, the permissions are treated as if the bits are zero.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx
[40]	RES0	Reserved	RES0
[39]	HA	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Hardware Access flag update in stage 1 translations from ELO and EL1.</p> <p><b>0b0</b></p> <p>Stage 1 Access flag update disabled.</p> <p><b>0b1</b></p> <p>Stage 1 Access flag update enabled.</p> <p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>RES0</p> <p><b>Otherwise</b></p> <p>RES0</p>	x

Bits	Name	Description	Reset
[38]	TBI1	<p><b>When AArch64-VTCR_EL2.MSA == '0'</b> RES0</p> <p><b>When AArch64-VTCR_EL2.MSA == '1'</b> Top Byte ignored. Indicates whether the top byte of an address is used for address match for the AArch64-TTBR1_EL1 region, or ignored and used for tagged addresses.</p> <p><b>0b0</b> Top Byte used in the address calculation.</p> <p><b>0b1</b> Top Byte ignored in the address calculation.</p> <p>This affects addresses generated in EL0 and EL1 using AArch64 where the address would be translated by tables pointed to by AArch64-TTBR1_EL1. It has an effect whether the EL1&amp;O translation regime is enabled or not.</p> <p>If FEAT_PAuth is implemented and TCR_EL1.TBID1 is 1, then this field only applies to Data accesses.</p> <p>Otherwise, if the value of TBI1 is 1 and bit [55] of the target address to be stored to the PC is 1, then bits[63:56] of that target address are also set to 1 before the address is stored in the PC, in the following cases:</p> <ul style="list-style-type: none"> <li>• A branch or procedure return within EL0 or EL1.</li> <li>• An exception taken to EL1.</li> <li>• An exception return to EL0 or EL1.</li> </ul> <p><b>Otherwise</b> RES0</p>	x



Bits	Name	Description	Reset
[37]	TBIO	<p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>Top Byte ignored. Indicates whether the top byte of an address is used for an address match for the EL1 MPU regions, or ignored and used for tagged addresses.</p> <p><b>0b0</b></p> <p>Top Byte used in the address calculation.</p> <p><b>0b1</b></p> <p>Top Byte ignored in the address calculation.</p> <p>This affects addresses generated in EL0 and EL1, where the address would be translated by the EL1 MPU.</p> <p>If FEAT_PAuth is implemented and TCR_EL1.TBID0 is 1, then this field only applies to Data accesses.</p> <p>Otherwise, if the value of TBIO is 1 and bit [55] of the target address to be stored to the PC is 0, then bits[63:56] of that target address are also set to 0 before the address is stored in the PC, in the following cases:</p> <ul style="list-style-type: none"> <li>• A branch or procedure return within EL0 or EL1.</li> <li>• An exception taken to EL1.</li> <li>• An exception return to EL0 or EL1.</li> </ul> <p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Top Byte ignored. Indicates whether the top byte of an address is used for address match for the AArch64-TTBRO_EL1 region, or ignored and used for tagged addresses.</p> <p><b>0b0</b></p> <p>Top Byte used in the address calculation.</p> <p><b>0b1</b></p> <p>Top Byte ignored in the address calculation.</p> <p>This affects addresses generated in EL0 and EL1 using AArch64 where the address would be translated by tables pointed to by AArch64-TTBRO_EL1. It has an effect whether the EL1&amp;O translation regime is enabled or not.</p> <p>If FEAT_PAuth is implemented and TCR_EL1.TBID0 is 1, then this field only applies to Data accesses.</p> <p>Otherwise, if the value of TBIO is 1 and bit [55] of the target address to be stored to the PC is 0, then bits[63:56] of that target address are also set to 0 before the address is stored in the PC, in the following cases:</p> <ul style="list-style-type: none"> <li>• A branch or procedure return within EL0 or EL1.</li> <li>• An exception taken to EL1.</li> <li>• An exception return to EL0 or EL1.</li> </ul> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx

Bits	Name	Description	Reset
[36]	AS	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>ASID Size.</p> <p><b>0b0</b></p> <p>8 bit - the upper 8 bits of AArch64-TTBR0_EL1 and AArch64-TTBR1_EL1 are ignored by hardware for every purpose except reading back the register, and are treated as if they are all zeros for when used for allocation and matching entries in the TLB.</p> <p><b>0b1</b></p> <p>16 bit - the upper 16 bits of AArch64-TTBR0_EL1 and AArch64-TTBR1_EL1 are used for allocation and matching in the TLB.</p> <p><b>When AArch64-VTCR_EL2.MSA == '0'</b></p> <p>ASID Size.</p> <p><b>0b0</b></p> <p>8 bit - the upper 8 bits of AArch64-TTBR0_EL1 are ignored by hardware for every purpose except reading back the register, and are treated as if they are all zeros when used for address matching.</p> <p><b>0b1</b></p> <p>16 bit - the upper 16 bits of AArch64-TTBR0_EL1 are used for address matching.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx
[35]	RES0	Reserved	RES0
[34:32]	IPS	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Intermediate Physical Address Size.</p> <p><b>0b000</b></p> <p>32 bits, 4GB.</p> <p><b>0b001</b></p> <p>36 bits, 64GB.</p> <p><b>0b010</b></p> <p>40 bits, 1TB.</p> <p><b>0b011</b></p> <p>42 bits, 4TB.</p> <p><b>0b100</b></p> <p>44 bits, 16TB.</p> <p><b>0b101</b></p> <p>48 bits, 256TB.</p> <p><b>0b110</b></p> <p>52 bits, 4PB.</p> <p>All other values are reserved.</p> <p>The reserved values behave in the same way as the 0b101 or 0b110 encoding, but software must not rely on this property as the behavior of the reserved values might change in a future revision of the architecture.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx

Bits	Name	Description	Reset
[31:30]	TG1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Granule size for the AArch64-TTBR1_EL1.</p> <p><b>0b01</b> 16KB.</p> <p><b>0b10</b> 4KB.</p> <p><b>0b11</b> 64KB.</p> <p>Other values are reserved.</p> <p>If the value is programmed to either a reserved value or a size that has not been implemented, then the hardware will treat the field as if it has been programmed to be 0b10 for all purposes other than the value read back from this register.</p> <p>The value read back is the value programmed.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[29:28]	SH1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Shareability attribute for memory associated with translation table walks using AArch64-TTBR1_EL1.</p> <p><b>0b00</b> Non-shareable.</p> <p><b>0b10</b> Outer Shareable.</p> <p><b>0b11</b> Inner Shareable.</p> <p>Other values are reserved. The effect of programming this field to a Reserved value is that behavior is <b>CONSTRAINED UNPREDICTABLE</b>.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[27:26]	ORGN1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Outer cacheability attribute for memory associated with translation table walks using AArch64-TTBR1_EL1.</p> <p><b>0b00</b> Normal memory, Outer Non-cacheable.</p> <p><b>0b01</b> Normal memory, Outer Write-Back Read-Allocate Write-Allocate Cacheable.</p> <p><b>0b10</b> Normal memory, Outer Write-Through Read-Allocate No Write-Allocate Cacheable.</p> <p><b>0b11</b> Normal memory, Outer Write-Back Read-Allocate No Write-Allocate Cacheable.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[25:24]	IRGN1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Inner cacheability attribute for memory associated with translation table walks using AArch64-TTBR1_EL1.</p> <p><b>0b00</b> Normal memory, Inner Non-cacheable.</p> <p><b>0b01</b> Normal memory, Inner Write-Back Read-Allocate Write-Allocate Cacheable.</p> <p><b>0b10</b> Normal memory, Inner Write-Through Read-Allocate No Write-Allocate Cacheable.</p> <p><b>0b11</b> Normal memory, Inner Write-Back Read-Allocate No Write-Allocate Cacheable.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[23]	EPD1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Translation table walk disable for translations using AArch64-TTBR1_EL1. This bit controls whether a translation table walk is performed on a TLB miss, for an address that is translated using AArch64-TTBR1_EL1. The encoding of this bit is:</p> <p><b>0b0</b> Perform translation table walks using AArch64-TTBR1_EL1.</p> <p><b>0b1</b> A TLB miss on an address that is translated using AArch64-TTBR1_EL1 generates a Translation fault. No translation table walk is performed.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[22]	A1	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Selects whether AArch64-TTBR0_EL1 or AArch64-TTBR1_EL1 defines the ASID. The encoding of this bit is:</p> <p><b>0b0</b> AArch64-TTBR0_EL1.ASID defines the ASID.</p> <p><b>0b1</b> AArch64-TTBR1_EL1.ASID defines the ASID.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[21:16]	T1SZ	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>The size offset of the memory region addressed by AArch64-TTBR1_EL1. The region size is <math>2^{(64-T1SZ)}</math> bytes.</p> <p>The maximum and minimum possible values for T1SZ depend on the level of translation table and the memory translation granule size, as described in the AArch64 Virtual Memory System Architecture chapter.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[15:14]	TG0	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Granule size for the AArch64-TTBRO_EL1.</p> <p><b>0b00</b> 4KB</p> <p><b>0b01</b> 64KB</p> <p><b>0b10</b> 16KB</p> <p>Other values are reserved.</p> <p>If the value is programmed to either a reserved value or a size that has not been implemented, then the hardware will treat the field as if it has been programmed to be 0b00 for all purposes other than the value read back from this register.</p> <p>The value read back is the value programmed.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[13:12]	SH0	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Shareability attribute for memory associated with translation table walks using AArch64-TTBRO_EL1.</p> <p><b>0b00</b> Non-shareable</p> <p><b>0b10</b> Outer Shareable</p> <p><b>0b11</b> Inner Shareable</p> <p>Other values are reserved. The effect of programming this field to a Reserved value is that behavior is <b>CONSTRAINED UNPREDICTABLE</b>.</p> <p><b>Otherwise</b> RES0</p>	xxxx
[11:10]	ORGN0	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Outer cacheability attribute for memory associated with translation table walks using AArch64-TTBRO_EL1.</p> <p><b>0b00</b> Normal memory, Outer Non-cacheable.</p> <p><b>0b01</b> Normal memory, Outer Write-Back Read-Allocate Write-Allocate Cacheable.</p> <p><b>0b10</b> Normal memory, Outer Write-Through Read-Allocate No Write-Allocate Cacheable.</p> <p><b>0b11</b> Normal memory, Outer Write-Back Read-Allocate No Write-Allocate Cacheable.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[9:8]	IRGNO	<b>When AArch64-VTCR_EL2.MSA == '1'</b> Inner cacheability attribute for memory associated with translation table walks using AArch64-TTBRO_EL1.  <b>0b00</b> Normal memory, Inner Non-cacheable.  <b>0b01</b> Normal memory, Inner Write-Back Read-Allocate Write-Allocate Cacheable.  <b>0b10</b> Normal memory, Inner Write-Through Read-Allocate No Write-Allocate Cacheable.  <b>0b11</b> Normal memory, Inner Write-Back Read-Allocate No Write-Allocate Cacheable.  <b>Otherwise</b> RES0	xxxx
[7]	EPDO	<b>When AArch64-VTCR_EL2.MSA == '1'</b> Translation table walk disable for translations using AArch64-TTBRO_EL1. This bit controls whether a translation table walk is performed on a TLB miss, for an address that is translated using AArch64-TTBRO_EL1. The encoding of this bit is:  <b>0b0</b> Perform translation table walks using AArch64-TTBRO_EL1.  <b>0b1</b> A TLB miss on an address that is translated using AArch64-TTBRO_EL1 generates a Translation fault. No translation table walk is performed.  <b>Otherwise</b> RES0	xxxx
[6]	RES0	Reserved	RES0
[5:0]	TOSZ	<b>When AArch64-VTCR_EL2.MSA == '1'</b> The size offset of the memory region addressed by AArch64-TTBRO_EL1. The region size is $2^{(64-TOSZ)}$ bytes. The maximum and minimum possible values for TOSZ depend on the level of translation table and the memory translation granule size, as described in the AArch64 Virtual Memory System Architecture chapter.  <b>Otherwise</b> RES0	xxxx

## Access

MRS <Xt>, TCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b010

MSR TCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0000	0b010

Accessibility

MRS <Xt>, TCR\_EL1


```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TCR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = TCR_EL1;
```

MSR TCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    TCR_EL1 = X[t, 64];
```

A.2.2.8 APIAKeyLo\_EL1, Pointer Authentication Key A for Instruction (bits[63:0])

Holds bits[63:0] of key A used for authentication of instruction pointer values.



Note

The term APIAKey\_EL1 is used to describe the concatenation of AArch64-APIAKeyHi\_EL1: AArch64-APIAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

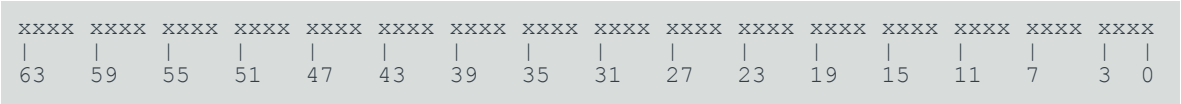
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-56: AARCH64\_APIAKEYLO\_EL1 bit assignments

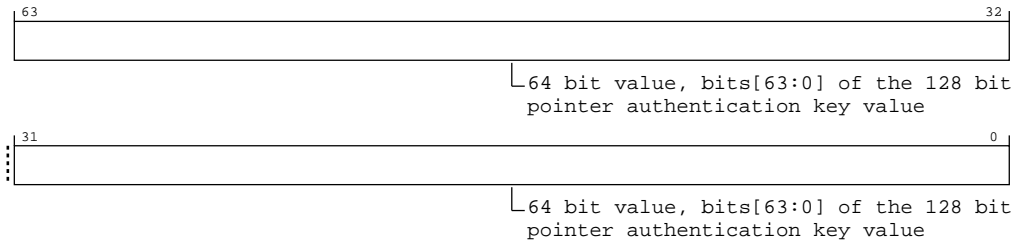


Table A-130: APIAKeyLo\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[63:0] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APIAKeyLo\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b000

MSR APIAKeyLo\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b000

Accessibility

MRS <Xt>, APIAKeyLo\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APIAKeyLo_EL1;
elseif PSTATE.EL == EL2 then
```



```
X[t, 64] = APIAKeyLo_EL1;
```

MSR APIAKeyLo\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APIAKeyLo_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    APIAKeyLo_EL1 = X[t, 64];
```

A.2.2.9 APIAKeyHi\_EL1, Pointer Authentication Key A for Instruction (bits[127:64])

Holds bits[127:64] of key A used for authentication of instruction pointer values.



The term APIAKey\_EL1 is used to describe the concatenation of AArch64-APIAKeyHi\_EL1: AArch64-APIAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-57: AARCH64\_APIAKEYHI\_EL1 bit assignments

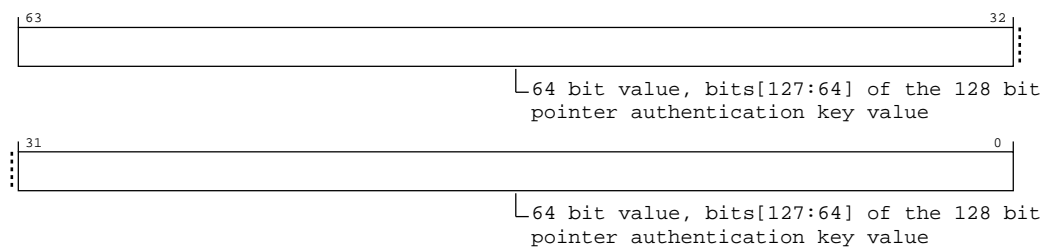


Table A-133: APIAKeyHi\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[127:64] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APIAKeyHi\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b001

MSR APIAKeyHi\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b001

Accessibility

MRS <Xt>, APIAKeyHi\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APIAKeyHi_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = APIAKeyHi_EL1;
```

MSR APIAKeyHi\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APIAKeyHi_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
```

```
APIAKeyHi_EL1 = X[t, 64];
```

A.2.2.10 APIBKeyLo\_EL1, Pointer Authentication Key B for Instruction (bits[63:0])

Holds bits[63:0] of key B used for authentication of instruction pointer values.



The term APIBKey\_EL1 is used to describe the concatenation of AArch64-APIBKeyHi\_EL1: AArch64-APIBKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

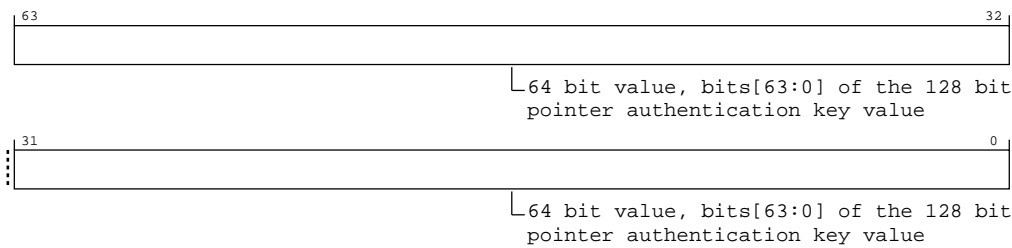
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-58: AARCH64\_APIBKEYLO\_EL1 bit assignments



**Table A-136: APIBKeyLo\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[63:0] of the 128 bit pointer authentication key value.	64 {x}

**Access**

MRS &lt;Xt&gt;, APIBKeyLo\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b010

MSR APIBKeyLo\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b010

**Accessibility**

MRS &lt;Xt&gt;, APIBKeyLo\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APIBKeyLo_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = APIBKeyLo_EL1;

```

MSR APIBKeyLo\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APIBKeyLo_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    APIBKeyLo_EL1 = X[t, 64];

```

**A.2.2.11 APIBKeyHi\_EL1, Pointer Authentication Key B for Instruction (bits[127:64])**

Holds bits[127:64] of key B used for authentication of instruction pointer values.

**Note**

The term APIBKey\_EL1 is used to describe the concatenation of AArch64-APIBKeyHi\_EL1: AArch64-APIBKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-59: AARCH64\_APIBKEYHI\_EL1 bit assignments

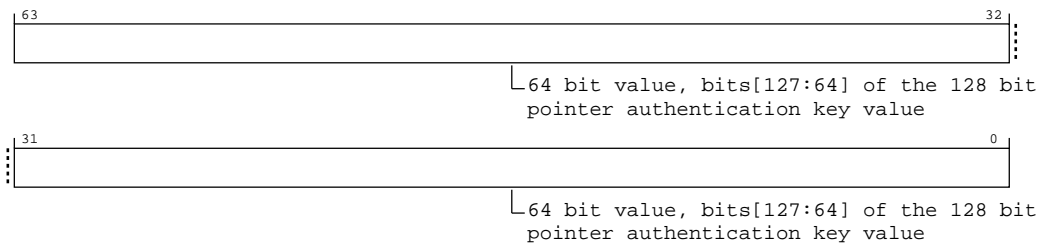


Table A-139: APIBKeyHi\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[127:64] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APIBKeyHi\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b011

MSR APIBKeyHi\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0001	0b011

Accessibility

MRS <Xt>, APIBKeyHi\_EL1


```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APIBKeyHi_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = APIBKeyHi_EL1;
```

MSR APIBKeyHi\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APIBKeyHi_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    APIBKeyHi_EL1 = X[t, 64];
```

A.2.2.12 APDAKeyLo\_EL1, Pointer Authentication Key A for Data (bits[63:0])

Holds bits[63:0] of key A used for authentication of data pointer values.



Note

The term APDAKey\_EL1 is used to describe the concatenation of AArch64-APDAKeyHi\_EL1: AArch64-APDAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-60: AARCH64\_APDAKEYLO\_EL1 bit assignments

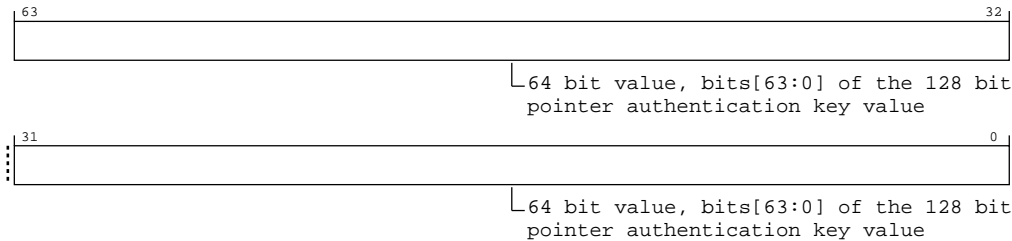


Table A-142: APDAKeyLo\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[63:0] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APDAKeyLo\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b000

MSR APDAKeyLo\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b000

Accessibility

MRS <Xt>, APDAKeyLo\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APDAKeyLo_EL1;
elseif PSTATE.EL == EL2 then
```

```
X[t, 64] = APDAKeyLo_EL1;
```

MSR APDAKeyLo\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APDAKeyLo_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    APDAKeyLo_EL1 = X[t, 64];
```

A.2.2.13 APDAKeyHi\_EL1, Pointer Authentication Key A for Data (bits[127:64])

Holds bits[127:64] of key A used for authentication of data pointer values.



The term APDAKey\_EL1 is used to describe the concatenation of AArch64-APDAKeyHi\_EL1: AArch64-APDAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-61: AARCH64\_APDAKEYHI\_EL1 bit assignments

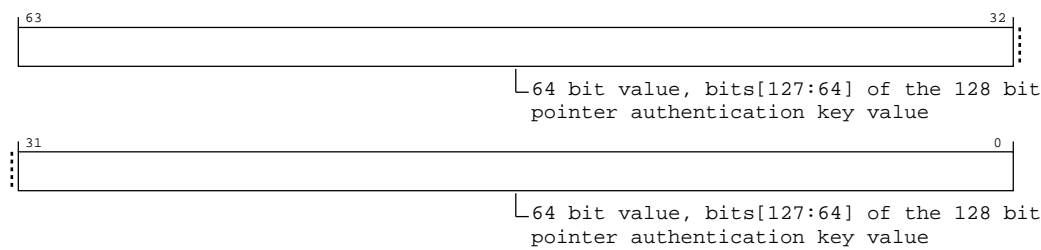


Table A-145: APDAKeyHi\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[127:64] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APDAKeyHi\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b001

MSR APDAKeyHi\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b001

Accessibility

MRS <Xt>, APDAKeyHi\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APDAKeyHi_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = APDAKeyHi_EL1;
```

MSR APDAKeyHi\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APDAKeyHi_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
```

```
APDAKeyHi_EL1 = X[t, 64];
```

A.2.2.14 APDBKeyLo\_EL1, Pointer Authentication Key B for Data (bits[63:0])

Holds bits[63:0] of key B used for authentication of data pointer values.



The term APDBKey\_EL1 is used to describe the concatenation of AArch64-APDBKeyHi\_EL1: AArch64-APDBKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

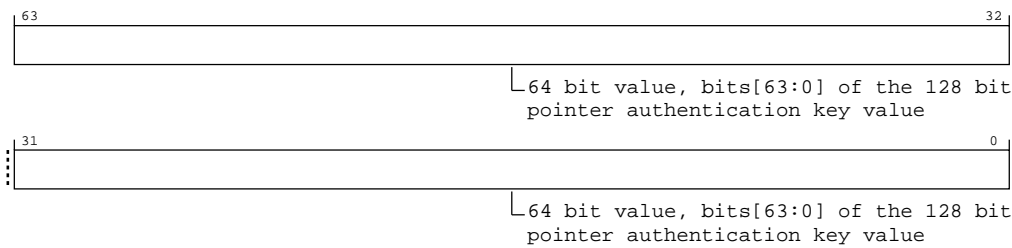
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-62: AARCH64\_APDBKEYLO\_EL1 bit assignments



**Table A-148: APDBKeyLo\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[63:0] of the 128 bit pointer authentication key value.	64 {x}

**Access**

MRS &lt;Xt&gt;, APDBKeyLo\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b010

MSR APDBKeyLo\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b010

**Accessibility**

MRS &lt;Xt&gt;, APDBKeyLo\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APDBKeyLo_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = APDBKeyLo_EL1;

```

MSR APDBKeyLo\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APDBKeyLo_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    APDBKeyLo_EL1 = X[t, 64];

```

**A.2.2.15 APDBKeyHi\_EL1, Pointer Authentication Key B for Data (bits[127:64])**

Holds bits[127:64] of key B used for authentication of data pointer values.

**Note**

The term APDBKey\_EL1 is used to describe the concatenation of AArch64-APDBKeyHi\_EL1: AArch64-APDBKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-63: AARCH64\_APDBKEYHI\_EL1 bit assignments

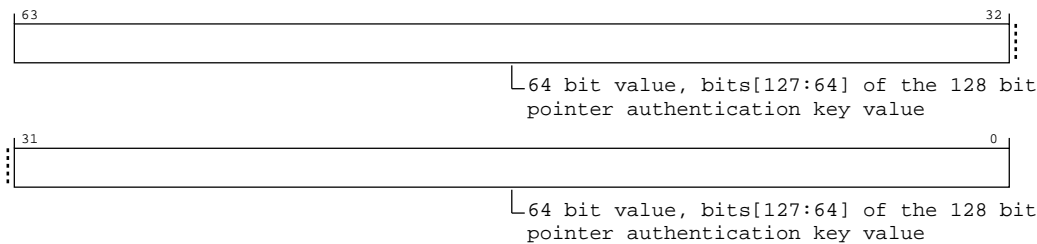


Table A-151: APDBKeyHi\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[127:64] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APDBKeyHi\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b011

MSR APDBKeyHi\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0010	0b011

Accessibility

MRS <Xt>, APDBKeyHi\_EL1


```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APDBKeyHi_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = APDBKeyHi_EL1;
```

MSR APDBKeyHi\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APDBKeyHi_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    APDBKeyHi_EL1 = X[t, 64];
```

A.2.2.16 APGAKeyLo\_EL1, Pointer Authentication Key A for Code (bits[63:0])

Holds bits[63:0] of key used for generic pointer authentication code.



Note

The term APGAKey\_EL1 is used to describe the concatenation of AArch64-APGAKeyHi\_EL1: AArch64-APGAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

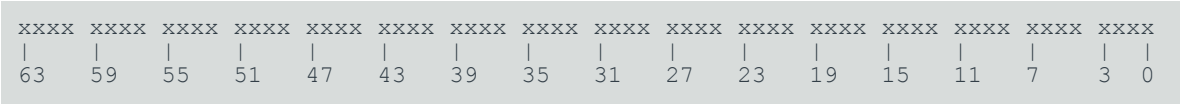
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-64: AARCH64\_APGAKEYLO\_EL1 bit assignments

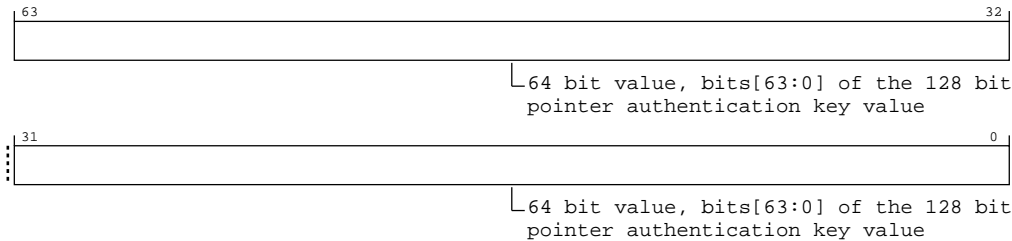


Table A-154: APGAKeyLo\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[63:0] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APGAKeyLo\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0011	0b000

MSR APGAKeyLo\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0011	0b000

Accessibility

MRS <Xt>, APGAKeyLo\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APGAKeyLo_EL1;
elseif PSTATE.EL == EL2 then
```

```
X[t, 64] = APGAKeyLo_EL1;
```

MSR APGAKeyLo\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APGAKeyLo_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    APGAKeyLo_EL1 = X[t, 64];
```

A.2.2.17 APGAKeyHi\_EL1, Pointer Authentication Key A for Code (bits[127:64])

Holds bits[127:64] of key used for generic pointer authentication code.



The term APGAKey\_EL1 is used to describe the concatenation of AArch64-APGAKeyHi\_EL1: AArch64-APGAKeyLo\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-65: AARCH64\_APGAKEYHI\_EL1 bit assignments

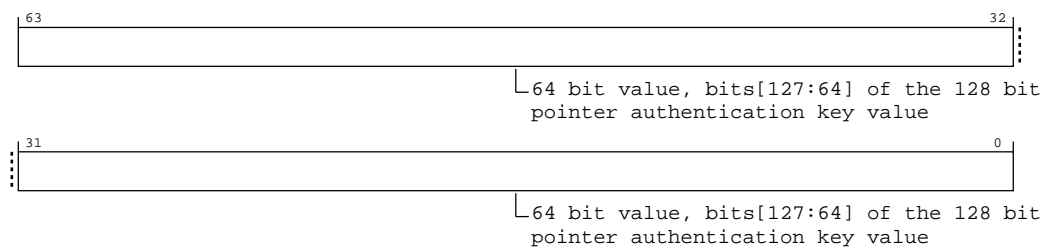


Table A-157: APGAKeyHi\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	64 bit value, bits[127:64] of the 128 bit pointer authentication key value.	64 {x}

Access

MRS <Xt>, APGAKeyHi\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0011	0b001

MSR APGAKeyHi\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0011	0b001

Accessibility

MRS <Xt>, APGAKeyHi\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = APGAKeyHi_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = APGAKeyHi_EL1;
```

MSR APGAKeyHi\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.APK == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        APGAKeyHi_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
```



```
APGAKeyHi_EL1 = X[t, 64];
```

A.2.2.18 SPSel, Stack Pointer Select

Allows the Stack Pointer to be selected between SP\_ELO and SP\_ELx.

Configurations

This register is available in all configurations.

Attributes

Width

64

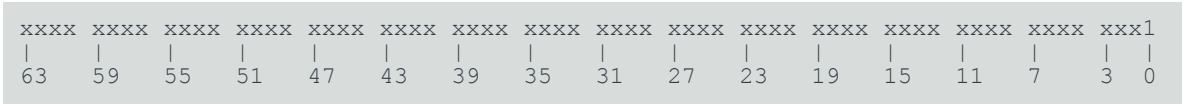
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-66: AARCH64\_SPSEL bit assignments

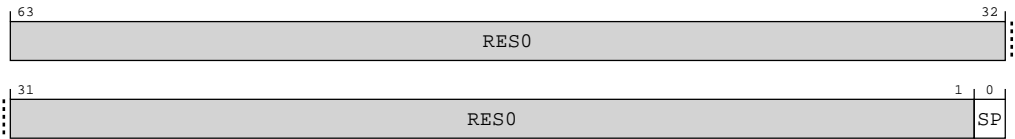


Table A-160: SPSel bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	SP	Stack pointer to use. Possible values of this bit are:  <b>0b0</b> Use SP_ELO at all Exception levels.  <b>0b1</b> Use SP_ELx for Exception level ELx.	0b1

Access

MRS <Xt>, SPSel

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b000

MSR SPSel, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b000

MSR SPSel, #<imm>

op0	op1	CRn	op2
0b00	0b000	0b0100	0b101

Accessibility

MRS <Xt>, SPSel

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(63):PSTATE.SP;
elsif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(63):PSTATE.SP;
```

MSR SPSel, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    PSTATE.SP = X[t, 64]<0>;
elsif PSTATE.EL == EL2 then
    PSTATE.SP = X[t, 64]<0>;
```

MSR SPSel, #<imm>

A.2.2.19 CurrentEL, Current Exception Level

Holds the current Exception level.

Configurations

This register is available in all configurations.

Attributes

Width

64

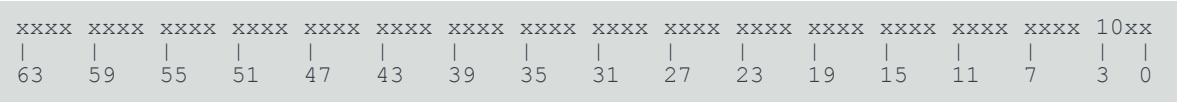
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-67: AARCH64\_CURRENTEL bit assignments

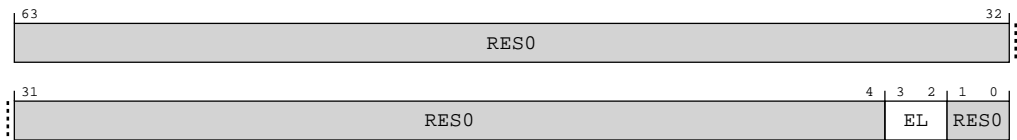


Table A-164: CurrentEL bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:2]	EL	Current Exception level.  0b00 EL0.  0b01 EL1.  0b10 EL2.	0b10

Bits	Name	Description	Reset
[1:0]	RES0	Reserved	RES0

**Access**  
MRS <Xt>, CurrentEL

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b010

**Accessibility**  
MRS <Xt>, CurrentEL

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(60):PSTATE.EL:Zeros(2);
elsif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(60):PSTATE.EL:Zeros(2);
```

A.2.2.20 PAN, Privileged Access Never

Allows access to the Privileged Access Never bit.

**Configurations**  
This register is available in all configurations.

**Attributes**

**Width**  
64

**Functional group**  
Generic System Control

**Access type**  
See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-68: AARCH64\_PAN bit assignments

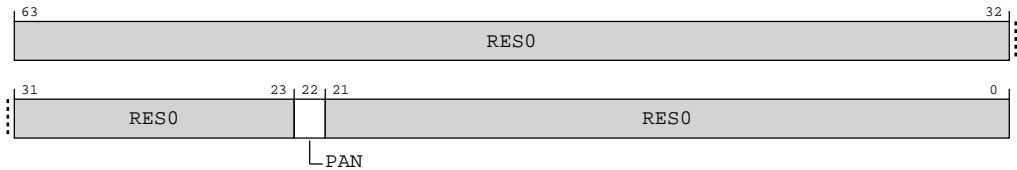


Table A-166: PAN bit descriptions

Bits	Name	Description	Reset
[63:23]	RES0	Reserved	RES0
[22]	PAN	Privileged Access Never.  <b>0b0</b> Privileged reads and write are not disabled by this mechanism.  <b>0b1</b> Disables privileged read and write accesses to addresses accessible at EL0 for an enabled stage 1 translation regime that defines the EL0 permissions.  The value of this bit is usually preserved on taking an exception, except in the following situations: <ul style="list-style-type: none"><li>When the target of the exception is EL1, and the value of the AArch64-SCTLR_EL1.SPAN bit is 0, this bit is set to 1.</li><li>When the target of the exception is EL2, AArch64-HCR_EL2.{E2H, TGE} is {1, 1}, and the value of the AArch64-SCTLR_EL2.SPAN bit is 0, this bit is set to 1.</li></ul>	x
[21:0]	RES0	Reserved	RES0

Access

MRS <Xt>, PAN

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b011

MSR PAN, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b011

MSR PAN, #<imm>

op0	op1	CRn	op2
0b00	0b000	0b0100	0b100

Accessibility

MRS <Xt>, PAN

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(41):PSTATE.PAN:Zeros(22);
elseif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(41):PSTATE.PAN:Zeros(22);
```

MSR PAN, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    PSTATE.PAN = X[t, 64]<22>;
elseif PSTATE.EL == EL2 then
    PSTATE.PAN = X[t, 64]<22>;
```

MSR PAN, #<imm>

A.2.2.21 UAO, User Access Override

Allows access to the User Access Override bit.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-69: AARCH64\_UAO bit assignments

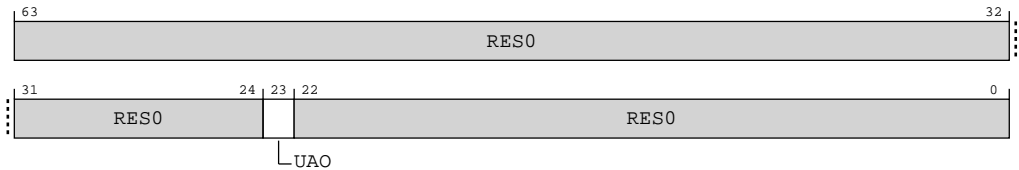


Table A-170: UAO bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23]	UAO	User Access Override.  <b>0b0</b> The behavior of LDTR* and STTR* instructions is as defined in the base Armv8 architecture.  <b>0b1</b> When executed at the following Exception levels, LDTR* and STTR* instructions behave as the equivalent LDR* and STR* instructions: <ul style="list-style-type: none"><li>EL1.</li></ul> When executed at EL2, the LDTR* and STTR* instructions behave as the equivalent LDR* and STR* instructions, regardless of the setting of the PSTATE.UAO bit.	x
[22:0]	RES0	Reserved	RES0

Access

For more information about the operation of the MSR (immediate) accessor, see *MSR (immediate)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

MRS <Xt>, UAO

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b100

MSR UAO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0010	0b100

MSR UAO, #<imm>

op0	op1	CRn	op2
0b00	0b000	0b0100	0b011

Accessibility

For more information about the operation of the MSR (immediate) accessor, see 'MSR (immediate)'.

MRS <Xt>, UAO

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(40):PSTATE.UAO:Zeros(23);
elseif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(40):PSTATE.UAO:Zeros(23);
```

MSR UAO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    PSTATE.UAO = X[t, 64]<23>;
elseif PSTATE.EL == EL2 then
    PSTATE.UAO = X[t, 64]<23>;
```

MSR UAO, #<imm>

A.2.2.22 AFSR0\_EL1, Auxiliary Fault Status Register 0 (EL1)

Provides additional implementation defined fault status information for Data Abort, Instruction Abort or SError interrupt taken to EL1

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-70: AARCH64\_AFSRO\_EL1 bit assignments

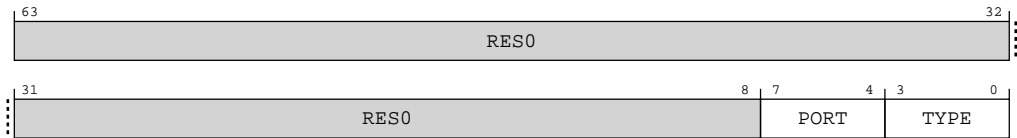


Table A-174: AFSRO\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:4]	PORT	Memory or bus interface that caused the abort.  <b>0b0000</b> MM. Main Manager port.  <b>0b0001</b> LLRAM. Low-Latency RAM port.  <b>0b0010</b> LLPP. Low-Latency Peripheral Port.  <b>0b0011</b> SPP. Shared Peripheral Port.  <b>0b0100</b> ITCM. Instruction Tightly Coupled Memory.  <b>0b0101</b> DTCM. Data Tightly Coupled Memory.  <b>0b0110</b> Overlapping or illegal port. Used for accesses that target multiple ports, when they simultaneously belong in two or more of the ITCM, DTCM, LLRAM, LLPP or SPP enabled regions. Also used for page table accesses if they belong in any of the ITCM, DTCM, LLRAM, LLPP or SPP enabled regions.  <b>0b0111</b> Unknown. All faults other than Instruction or Data aborts will have this type. For External aborts and Unsupported Exclusive or Atomic access faults, this is used for ambiguous memory accesses or for faults that do not have an associated address. For other Instruction or Data aborts, this indicates that the port information is not applicable to the fault.  <b>0b1000</b> SEI. System abort signaled by System Error Interrupt input pins.  Other values are Reserved.	xxxx

Bits	Name	Description	Reset
[3:0]	TYPE	Fault type.  <b>0b0000</b> Error on data.  <b>0b0001</b> Timeout error.  <b>0b0010</b> Error on interrupt latency. Indicates the abort was generated by an instruction trapped by AArch64-IMP_INTLATENCY_EL2 controls.  <b>0b0011</b> Other error.  Other values are Reserved.	xxxx

Access

MRS <Xt>, AFSRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0001	0b000

MSR AFSRO\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0001	0b000

Accessibility

MRS <Xt>, AFSRO\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = AFSRO_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = AFSRO_EL1;
```

MSR AFSRO\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AFSRO_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    AFSRO_EL1 = X[t, 64];
```

### A.2.2.23 AFSR1\_EL1, Auxiliary Fault Status Register 1 (EL1)

Provides additional **IMPLEMENTATION DEFINED** fault status information for exceptions taken to EL1.

## Configurations

This register is available in all configurations.

## Attributes

## Width

64

## Functional group

## Generic System Control

### Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

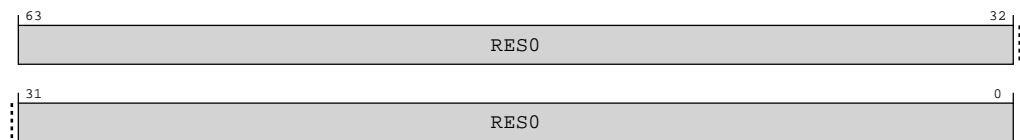


## Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure A-71: AARCH64\_AFSR1\_EL1 bit assignments



### Table A-177: AFSR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

## Access

MRS &lt;Xt&gt;, AFSR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0001	0b001

MSR AFSR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0001	0b001

Accessibility

MRS <Xt>, AFSR1\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = AFSR1_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = AFSR1_EL1;
```

MSR AFSR1\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AFSR1_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    AFSR1_EL1 = X[t, 64];
```

A.2.2.24 ESR\_EL1, Exception Syndrome Register (EL1)

Holds syndrome information for an exception taken to EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

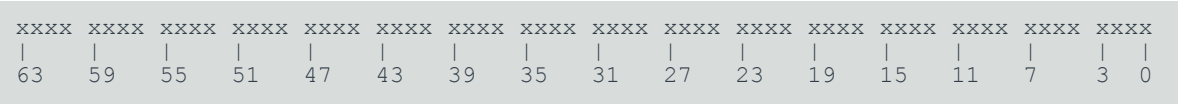
Functional group

Generic System Control

Access type

See bit descriptions

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

ESR\_EL1 is made **UNKNOWN** as a result of an exception return from EL1.

When an UNPREDICTABLE instruction is treated as UNDEFINED, and the exception is taken to EL1, the value of ESR\_EL1 is **UNKNOWN**. The value written to ESR\_EL1 must be consistent with a value that could be created as a result of an exception from the same Exception level that generated the exception as a result of a situation that is not UNPREDICTABLE at that Exception level, in order to avoid the possibility of a privilege violation.

Figure A-72: AARCH64\_ESR\_EL1 bit assignments

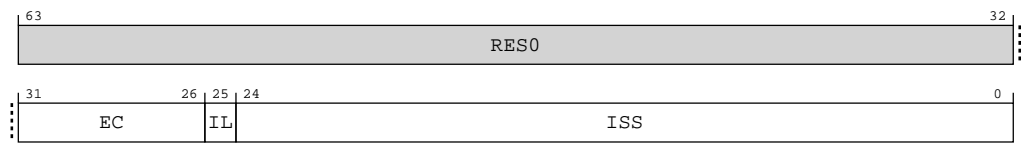


Table A-180: ESR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:26]	EC	<p>Exception Class. Indicates the reason for the exception that this register holds information about.</p> <p>For each EC value, the table references a subsection that gives information about:</p> <ul style="list-style-type: none"><li>The cause of the exception, for example the configuration required to enable the trap.</li><li>The encoding of the associated ISS.</li></ul> <p>Possible values of the EC field are:</p> <p><b>0b000000</b> Unknown reason.</p> <p><b>0b000001</b> Trapped WFI or WFE instruction execution.</p> <p>Conditional WFE and WFI instructions that fail their condition code check do not cause an exception.</p> <p><b>0b000111</b> Access to Advanced SIMD, or floating-point functionality trapped by AArch64-CPACR_EL1.FPEN, AArch64-CPTR_EL2.FPEN, or AArch64-CPTR_EL2.TFP control.</p> <p>Excludes exceptions resulting from AArch64-CPACR_EL1 when the value of AArch64-HCR_EL2.TGE is 1, or because Advanced SIMD and floating-point are not implemented. These are reported with EC value 0b000000.</p> <p><b>0b001110</b> Illegal Execution state.</p>	6 {x}

Bits	Name	Description	Reset
[31:26 continued]	EC	<p><b>0b010101</b> SVC instruction execution in AArch64 state.</p> <p><b>0b011000</b> Trapped MSR, MRS or System instruction execution in AArch64 state, that is not reported using EC 0b000000, 0b000001 or 0b000111.</p> <p>This includes all instructions that cause exceptions that are part of the encoding space defined 'System instruction class encoding overview', except for those exceptions reported using EC values 0b000000, 0b000001, or 0b000111.</p> <p><b>0b011100</b> Exception from a Pointer Authentication instruction authentication failure</p> <p><b>0b100000</b> Instruction Abort from a lower Exception level.</p> <p>Used for MMU faults generated by instruction accesses and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p>	6{x}
[31:26 continued]	EC	<p><b>0b100001</b> Instruction Abort taken without a change in Exception level.</p> <p>Used for MMU faults generated by instruction accesses and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100010</b> PC alignment fault exception.</p> <p><b>0b100100</b> Data Abort from a lower Exception level.</p> <p>Used for MMU faults generated by data accesses, alignment faults other than those caused by Stack Pointer misalignment, and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100101</b> Data Abort taken without a change in Exception level.</p> <p>Used for MMU faults generated by data accesses, alignment faults other than those caused by Stack Pointer misalignment, and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100110</b> SP alignment fault exception.</p> <p><b>0b101111</b> SError interrupt.</p> <p><b>0b110000</b> Breakpoint exception from a lower Exception level.</p>	6{x}

Bits	Name	Description	Reset
[31:26 continued]	EC	<p><b>0b110001</b> Breakpoint exception taken without a change in Exception level.</p> <p><b>0b110010</b> Software Step exception from a lower Exception level.</p> <p><b>0b110011</b> Software Step exception taken without a change in Exception level.</p> <p><b>0b110100</b> Watchpoint exception from a lower Exception level.</p> <p><b>0b110101</b> Watchpoint exception taken without a change in Exception level.</p> <p><b>0b111100</b> BRK instruction execution in AArch64 state.</p> <p>All other EC values are reserved by Arm, and:</p> <ul style="list-style-type: none"> <li>Unused values in the range 0b000000 - 0b101100 (0x00 - 0x2C) are reserved for future use for synchronous exceptions.</li> <li>Unused values in the range 0b101101 - 0b111111 (0x2D - 0x3F) are reserved for future use, and might be used for synchronous or asynchronous exceptions.</li> </ul> <p>The effect of programming this field to a reserved value is that behavior is <b>CONSTRAINED UNPREDICTABLE</b>.</p>	6 {x}
[25]	IL	<p>Instruction Length for synchronous exceptions. Possible values of this bit are:</p> <p><b>0b0</b> 16-bit instruction trapped.</p> <p><b>0b1</b> 32-bit instruction trapped. This value is also used when the exception is one of the following:</p> <ul style="list-style-type: none"> <li>An SError interrupt.</li> <li>An Instruction Abort exception.</li> <li>A PC alignment fault exception.</li> <li>An SP alignment fault exception.</li> <li>A Data Abort exception for which the value of the ISV bit is 0.</li> <li>An Illegal Execution state exception.</li> <li>Any debug exception except for Breakpoint instruction exceptions. For Breakpoint instruction exceptions, this bit has its standard meaning: <ul style="list-style-type: none"> <li>0b1: 32-bit A64 BRK instruction.</li> </ul> </li> <li>An exception reported using EC value 0b000000.</li> </ul>	x
[24:0]	ISS	<p><b>ISS encoding for exceptions with an unknown reason</b></p> <p><b>24:0</b> Reserved, <b>RES0</b>.</p> <p>When an exception is reported using this EC code the IL field is set to 1.</p> <p>This EC code is used for all exceptions that are not covered by any other EC value. This includes exceptions that are generated in the following situations:</p>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>The attempted execution of an instruction bit pattern that has no allocated instruction or that is not accessible at the current Exception level and Security state, including: <ul style="list-style-type: none"> <li>A read access using a System register pattern that is not allocated for reads or that does not permit reads at the current Exception level and Security state.</li> <li>A write access using a System register pattern that is not allocated for writes or that does not permit writes at the current Exception level and Security state.</li> <li>Instruction encodings that are unallocated.</li> <li>Instruction encodings for instructions or System registers that are not implemented in the implementation.</li> </ul> </li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>In Debug state, the attempted execution of an instruction bit pattern that is not accessible in Debug state.</li> <li>In Non-debug state, the attempted execution of an instruction bit pattern that is not accessible in Non-debug state.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>In an implementation that does not include Advanced SIMD and floating-point functionality, an attempted access to Advanced SIMD or floating-point functionality under conditions where that access would be permitted if that functionality was present. This includes the attempted execution of an Advanced SIMD or floating-point instruction, and attempted accesses to Advanced SIMD and floating-point System registers.</li> <li>Attempted execution of: <ul style="list-style-type: none"> <li>An HVC instruction when disabled by AArch64-HCR_EL2.HCD.</li> <li>An SMC instruction.</li> <li>An HLT instruction when disabled by ext-EDSCR.HDE.</li> </ul> </li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>Attempted execution of an MSR or MRS instruction to access AArch64-SP_ELO when the value of AArch64-SPSel.SP is 0.</li> <li>Attempted execution of an MSR or MRS instruction using a _EL12 register name.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>Attempted execution, in Debug state, of: <ul style="list-style-type: none"> <li>A DCPS1 instruction when the value of AArch64-HCR_EL2.TGE is 1 and EL2 is disabled or not implemented in the current Security state.</li> <li>A DCPS2 instruction from EL1 or EL0 when EL2 is disabled or not implemented in the current Security state.</li> <li>A DCPS3 instruction</li> </ul> </li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>An exception that is taken to EL2 because the value of AArch64-HCR_EL2.TGE is 1 that, if the value of AArch64-HCR_EL2.TGE was 0 would have been reported with an ESR_ELx.EC value of 0b000111.</li> </ul>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from a WF* instruction</b></p> <p><b>24</b></p> <p>Condition code valid.</p> <p><b>0b0</b></p> <p>The COND field is not valid.</p> <p><b>0b1</b></p> <p>The COND field is valid.</p> <p><b>23:20</b></p> <p>For exceptions taken from AArch64, this field is set to 0b1110.</p>	25 {x}



Bits	Name	Description	Reset
[24:0 continued]	ISS	<p><b>19:2</b></p> <p>Reserved, <b>RES0</b>.</p> <p><b>1:0</b></p> <p>Trapped instruction. Possible values of this bit are:</p> <p><b>0b00</b></p> <p>WFI trapped.</p> <p><b>0b01</b></p> <p>WFE trapped.</p> <p>The following fields describe configuration settings for generating this exception:</p> <ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.{nTWE, nTWI}.</li> <li>AArch64-HCR_EL2.{TWE, TWI}.</li> </ul>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from an access to SVE, Advanced SIMD or floating-point functionality, resulting from the FPEN and TFP traps</b></p> <p>The accesses covered by this trap include:</p> <ul style="list-style-type: none"> <li>Execution of SVE or Advanced SIMD and floating-point instructions.</li> <li>Accesses to the Advanced SIMD and floating-point System registers.</li> </ul> <p>For an implementation that does not include either SVE or support for Advanced SIMD and floating-point, the exception is reported using the EC value 0b000000.</p>	25 {x}
[24:0 continued]	ISS	<p><b>24</b></p> <p>Condition code valid.</p> <p><b>0b0</b></p> <p>The COND field is not valid.</p> <p><b>0b1</b></p> <p>The COND field is valid.</p>	25 {x}
[24:0 continued]	ISS	<p><b>23:20</b></p> <p>For exceptions taken from AArch64, this field is set to 0b1110.</p> <p><b>19:0</b></p> <p>Reserved, <b>RES0</b>.</p> <p>The following fields describe the configuration settings for the traps that are reported using EC value 0b000111:</p> <ul style="list-style-type: none"> <li>AArch64-CPACR_EL1.FPEN, for accesses to SIMD and floating-point registers trapped to EL1.</li> <li>AArch64-CPTR_EL2.FPEN and AArch64-CPTR_EL2.TFP, for accesses to SIMD and floating-point registers trapped to EL2.</li> </ul>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>ISS encoding for an exception from an Illegal Execution state, or a PC or SP alignment fault</b> <b>24:0</b> Reserved, <b>RES0</b> . <p>There are no configuration settings for generating Illegal Execution state exceptions and PC alignment fault exceptions. For more information about PC alignment fault exceptions, see <i>PC alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><i>SP alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> describes the configuration settings for generating SP alignment fault exceptions.</p>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from HVC or SVC instruction execution</b> <b>24:16</b> Reserved, <b>RES0</b> . <p>For A64 instructions, see SVC in the and 'HVC'.</p>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from MSR, MRS, or System instruction execution in AArch64 state</b> <b>24:22</b> Reserved, <b>RES0</b> . <b>21:20</b> The Op0 value from the issued instruction. <b>19:17</b> The Op2 value from the issued instruction.	25 {x}
[24:0 continued]	ISS	<b>16:14</b> The Op1 value from the issued instruction. <b>13:10</b> The CRn value from the issued instruction. <b>9:5</b> The Rt value from the issued instruction, the general-purpose register used for the transfer.	25 {x}
[24:0 continued]	ISS	<b>4:1</b> The CRm value from the issued instruction. <b>0</b> Indicates the direction of the trapped instruction. <b>0b0</b> Write access, including MSR instructions. <b>0b1</b> Read access, including MRS instructions	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<p>For exceptions caused by System instructions, see <i>System instructions' subsection of 'Branches, exception generating and System instructions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> for the encoding values returned by an instruction.</p> <p>The following fields describe configuration settings for generating the exception that is reported using EC value 0b011000:</p> <ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.UCI, for execution of cache maintenance instructions using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-SCTLR_EL1.UCT, for accesses to AArch64-CTR_EL0 using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.DZE, for execution of DC ZVA instructions using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-SCTLR_EL1.UMA, for accesses to the PSTATE interrupt masks using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-CPACR_EL1.TTA, for accesses to the trace registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-MDSCR_EL1.TDCC, for accesses to the Debug Communications Channel (DCC) registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-CNTKCTL_EL1.{ELOPTEN, ELOVTEN, ELOPCTEN, ELOVCTEN} accesses to the Generic Timer registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-PMUSERENR_EL0.{ER, CR, SW, EN}, for accesses to the Performance Monitor registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-HCR_EL2.{TRVM, TVM}, for accesses to virtual memory control registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TDZ, for execution of DC ZVA instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.TTLB, for execution of TLB maintenance instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.{TSW, TPC, TPU}, for execution of cache maintenance instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TACR, for accesses to the Auxiliary Control Register, AArch64-ACTLR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TIDCP, for accesses to lockdown, DMA, and TCM operations using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.{TID1, TID2, TID3}, for accesses to ID group 1, ID group 2 or ID group 3 registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-CPTR_EL2.TCPAC, for accesses to AArch64-CPACR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-CPTR_EL2.TTA, for accesses to the trace registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TTRF, for accesses to the trace filter control register, AArch64-TRFCR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-MDCR_EL2.TDRA, for accesses to Debug ROM registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TDOSA, for accesses to powerdown debug registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-CNTHCTL_EL2.{EL1PCEN, EL1PCTEN}, for accesses to the Generic Timer registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TDA, for accesses to debug registers using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-MDCR_EL2.{TPM, TPMCR}, for accesses to Performance Monitor registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.APK, for accesses to Pointer authentication key registers. using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.AT, for execution of AT S1E* instructions, using AArch64 state, MSR or MRS access, trapped to EL2.</li> <li>AArch64-HCR_EL2.{TERR, FIEN}, for accesses to RAS registers, using AArch64 state, MSR or MRS access, trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from an Instruction Abort</b> <b>24:13</b> Reserved, <b>RES0</b> .	25 {x}
[24:0 continued]	ISS	<b>12:11</b> Synchronous Error Type. When IFSC is 0b010000, describes the PE error state after taking the Instruction Abort exception. <b>0b00</b> Recoverable state (UER). <b>0b10</b> Uncontainable (UC). <b>0b11</b> Restartable state (UEO).	25 {x}
[24:0 continued]	ISS	<b>10</b> FAR not Valid, for a synchronous External abort other than a synchronous External abort on a translation table walk. <b>0b0</b> FAR is valid. <b>0b1</b> FAR is not valid, and holds an UNKNOWN value. <b>9</b> External abort type. <b>0b0</b> No IMPLEMENTATION DEFINED classification of External aborts.	25 {x}
[24:0 continued]	ISS	<b>8</b> Cache maintenance. Indicates whether the Data Abort came from a cache maintenance or address translation instruction: <b>0b0</b> The Data Abort was not generated by the execution of one of the System instructions identified in the description of value 1.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>0b1</b> The Data Abort was generated by either the execution of a cache maintenance instruction or by a synchronous fault on the execution of an address translation instruction. The r[DC ZVA](AArch64-dc-zva), r[DC GVA](AArch64-dc-gva), and r[DC GZVA](AArch64-dc-gzva) instructions are not classified as cache maintenance instructions, and therefore their execution cannot cause this field to be set to 1.	25 {x}
[24:0 continued]	ISS	<b>7</b> For a stage 2 fault, indicates whether the fault was a stage 2 fault on an access made for a stage 1 translation table walk: <b>0b0</b> Fault not on a stage 2 translation for a stage 1 translation table walk. <b>0b1</b> Fault on the stage 2 translation of an access for a stage 1 translation table walk.	25 {x}
[24:0 continued]	ISS	<b>6</b> Write not Read. Indicates whether a synchronous abort was caused by an instruction writing to a memory location, or by an instruction reading from a memory location. <b>0b0</b> Abort caused by an instruction reading from a memory location. <b>0b1</b> Abort caused by an instruction writing to a memory location.	25 {x}
[24:0 continued]	ISS	<b>5:0</b> Data Fault Status Code. <b>0b000000</b> Address size fault, level 0 of translation or translation table base register. <b>0b000001</b> Address size fault, level 1.	25 {x}
[24:0 continued]	ISS	<b>0b000010</b> Address size fault, level 2. <b>0b000011</b> Address size fault, level 3. <b>0b000100</b> Translation fault, level 0. <b>0b000101</b> Translation fault, level 1. <b>0b000110</b> Translation fault, level 2. <b>0b000111</b> Translation fault, level 3.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>0b001001</b> Access flag fault, level 1.  <b>0b001010</b> Access flag fault, level 2.  <b>0b001011</b> Access flag fault, level 3.  <b>0b001100</b> Permission fault, level 0.  <b>0b001101</b> Permission fault, level 1.	25 {x}
[24:0 continued]	ISS	<b>0b001110</b> Permission fault, level 2.  <b>0b001111</b> Permission fault, level 3.  <b>0b010000</b> Synchronous External abort, not on translation table walk or hardware update of translation table.  <b>0b010100</b> Synchronous External abort on translation table walk or hardware update of translation table, level 0.	25 {x}
[24:0 continued]	ISS	<b>0b010101</b> Synchronous External abort on translation table walk or hardware update of translation table, level 1.  <b>0b010110</b> Synchronous External abort on translation table walk or hardware update of translation table, level 2.  <b>0b010111</b> Synchronous External abort on translation table walk or hardware update of translation table, level 3.	25 {x}
[24:0 continued]	ISS	<b>0b100001</b> Alignment fault.  <b>0b110000</b> TLB conflict abort.  <b>0b110001</b> Unsupported atomic hardware update fault.  <b>0b110100</b> IMPLEMENTATION DEFINED fault (Lockdown).  <b>0b110101</b> IMPLEMENTATION DEFINED fault (Unsupported Exclusive or Atomic access).	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an SError interrupt</b> <b>24</b> <b>IMPLEMENTATION DEFINED</b> syndrome. <b>0b0</b> Bits [23:0] of the ISS field holds the fields described in this encoding.  <b>0b1</b> Bits [23:0] of the ISS field holds IMPLEMENTATION DEFINED syndrome information that can be used to provide additional information about the SError interrupt.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>23:14</b> Reserved, <b>RES0</b> .  <b>13</b> Implicit error synchronization event.  <b>0b0</b> The SError interrupt was either not synchronized by the implicit error synchronization event or not taken immediately.  <b>0b1</b> The SError interrupt was synchronized by the implicit error synchronization event and taken immediately.	25 {x}
[24:0 continued]	ISS	<b>12:10</b> Asynchronous Error Type.  When DFSC is 0b010001, describes the PE error state after taking the SError interrupt exception.  <b>0b000</b> Uncontainable (UC).  <b>0b001</b> Unrecoverable state (UEU).  <b>0b010</b> Restartable state (UEO).  <b>0b011</b> Recoverable state (UER).  <b>0b110</b> Corrected (CE).	25 {x}
[24:0 continued]	ISS	<b>9</b> External abort type. When DFSC is 0b010001, provides an IMPLEMENTATION DEFINED classification of External aborts.  This field is valid only if the DFSC code is 0b010001. It is <b>RES0</b> for all other errors.  <b>8:6</b> Reserved, <b>RES0</b> .  <b>5:0</b> Data Fault Status Code.  <b>0b000000</b> Uncategorized error.  <b>0b010001</b> Asynchronous SError interrupt.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Breakpoint or Vector Catch debug exception</b>  <b>24:6</b> Reserved, RES0.  <b>5:0</b> Instruction Fault Status Code.  <b>0b100010</b> Debug exception.  For more information about generating these exceptions: <ul style="list-style-type: none"> <li>For exceptions from AArch64, see <i>Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</li> </ul>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Software Step exception</b>  <b>24</b> Instruction syndrome valid. Indicates whether the EX bit, ISS[6], is valid, as follows:  <b>0b0</b> EX bit is RES0.  <b>0b1</b> EX bit is valid.  <b>23:7</b> Reserved, RES0.	25 {x}
[24:0 continued]	ISS	<b>6</b> Exclusive operation. If the ISV bit is set to 1, this bit indicates whether a Load-Exclusive instruction was stepped.  <b>0b0</b> An instruction other than a Load-Exclusive instruction was stepped.  <b>0b1</b> A Load-Exclusive instruction was stepped.  <b>5:0</b> Instruction Fault Status Code.  <b>0b100010</b> Debug exception.  For more information about generating these exceptions, see <i>Software Step exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Watchpoint exception</b>  <b>24:9</b> Reserved, RES0.	25 {x}



Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>8</b> Cache maintenance. Indicates whether the Watchpoint exception came from a cache maintenance or address translation instruction: <b>0b0</b> The Watchpoint exception was not generated by the execution of one of the System instructions identified in the description of value 1. <b>0b1</b> The Watchpoint exception was generated by either the execution of a cache maintenance instruction or by a synchronous Watchpoint exception on the execution of an address translation instruction. The r[DC ZVA](AArch64-dc-zva), r[DC GVA](AArch64-dc-gva), and r[DC GZVA](AArch64-dc-gzva) instructions are not classified as a cache maintenance instructions, and therefore their execution cannot cause this field to be set to 1	25 {x}
[24:0 continued]	ISS	<b>7</b> Reserved, <b>RES0</b> . <b>6</b> Write not Read. Indicates whether the Watchpoint exception was caused by an instruction writing to a memory location, or by an instruction reading from a memory location. <b>0b0</b> Watchpoint exception caused by an instruction reading from a memory location. <b>0b1</b> Watchpoint exception caused by an instruction writing to a memory location. <b>5:0</b> Data Fault Status Code. <b>0b100010</b> Debug exception. For more information about generating these exceptions, see <i>Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from execution of a Breakpoint instruction</b> <b>24:16</b> Reserved, <b>RES0</b> . <b>15:0</b> Set to the instruction comment field value, zero extended as necessary. For more information about generating these exceptions, see <i>Breakpoint instruction exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Pointer Authentication instruction authentication failure</b>  <b>24:2</b> Reserved, <b>RES0</b> .  <b>1</b> This field indicates whether the exception is as a result of an Instruction key or a Data key. <b>0b0</b> Instruction Key. <b>0b1</b> Data Key.  <b>0</b> This field indicates whether the exception is as a result of an A key or a B key. <b>0b0</b> A key. <b>0b1</b> B key	25 {x}
[24:0 continued]	ISS	The following instructions generate an exception when the Pointer Authentication Code (PAC) is incorrect: <ul style="list-style-type: none"> <li>AUTIASP, AUTIAZ, AUTIA1716.</li> <li>AUTIBSP, AUTIBZ, AUTIB1716.</li> <li>AUTIA, AUTDA, AUTIB, AUTDB.</li> <li>AUTIZA, AUTIZB, AUTDZA, AUTDZB.</li> <li>RETAA, RETAB.</li> <li>BRAA, BRAB, BLRAA, BLRAB.</li> <li>BRAAZ, BRABZ, BLRAAZ, BLRABZ.</li> <li>ERETAA, ERETAB.</li> <li>LDRAA, LDRAB, whether the authenticated address is written back to the base register or not.</li> </ul>	25 {x}

## Access

MRS <Xt>, ESR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0010	0b000

MSR ESR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0010	0b000

## Accessibility

MRS <Xt>, ESR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ESR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ESR_EL1;
```

MSR ESR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ESR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ESR_EL1 = X[t, 64];
```

A.2.2.25 PRBAR<n>\_EL1, Protection Region Base Address Register n (EL1), n = 1 - 15

Provides access to the base address for the MPU region determined by the value of 'n' and AArch64-PRSELR\_EL1.REGION as AArch64-PRSELR\_EL1.REGION<7:4>:n.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

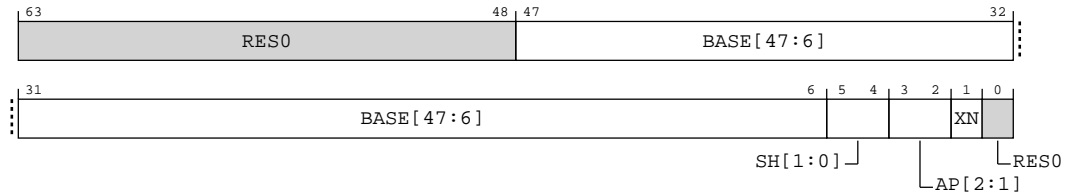
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-73: AARCH64\_PRBAR<n>\_EL1 bit assignments**



**Table A-183: PRBAR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	BASE[47:6]	Bits[47:6] of the lower inclusive limit of the selected EL1 MPU memory region. This value is zero extended to provide the base address to be checked against.	42 {x}
[5:4]	SH[1:0]	Shareability attribute.  <b>0b00</b> Non-shareable <b>0b01</b> Reserved, <b>CONSTRAINED UNPREDICTABLE</b> <b>0b10</b> Outer Shareable <b>0b11</b> Inner Shareable	xx
[3:2]	AP[2:1]	Access Permission attributes.  <b>0b00</b> Read/write at EL1, no access at ELO <b>0b01</b> Read/write at EL1 and ELO <b>0b10</b> Read-only at EL1, no access at ELO <b>0b11</b> Read-only at EL1 and ELO	xx
[1]	XN	Execute Never  <b>0b0</b> Execution of instructions fetched from the region is permitted. <b>0b1</b> Execution of instructions fetched from the region is not permitted.	x
[0]	RES0	Reserved	RES0

## Access

Any access to MPU region register PRBAR<n>\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRBAR<n>\_EL1 return an **UNKNOWN** value.
- Writes to unimplemented PRBAR<n>\_EL1 register make all PRBAR\_EL1 registers value **UNKNOWN**.

MRS <Xt>, PRBAR<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	'1':m[3:1]	m[0]:'00'

MSR PRBAR<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	'1':m[3:1]	m[0]:'00'

Accessibility

Any access to MPU region register PRBAR<n>\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRBAR<n>\_EL1 return an UNKNOWN value.
- Writes to unimplemented PRBAR<n>\_EL1 register make all PRBAR\_EL1 registers value UNKNOWN.

MRS <Xt>, PRBAR<m>\_EL1

```
integer m = UInt(CRm<2:0>:op2<2>);

if m + (UInt(PRSELR_EL1.REGION<7:4>) * 16) >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        X[t, 64] = PRBAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)];
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRBAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)];
```

MSR PRBAR<m>\_EL1, <Xt>

```
integer m = UInt(CRm<2:0>:op2<2>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
```

```
else
    PRBAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)] = X[t, 64];
elseif PSTATE.EL == EL2 then
    PRBAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)] = X[t, 64];
```

A.2.2.26 PRLAR<n>\_EL1, Protection Region Limit Address Register n (EL1), n = 1 - 15

Provides access to the limit address for the MPU region determined by the value of 'n' and AArch64-PRSELR\_EL1.REGION as AArch64-PRSELR\_EL1.REGION<7:4>:n.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

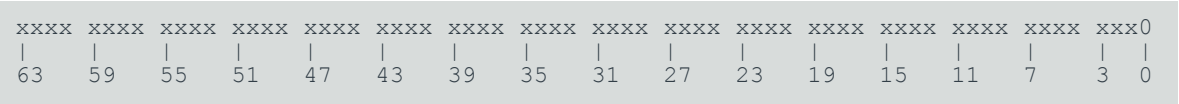
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-74: AARCH64\_PRLAR<n>\_EL1 bit assignments

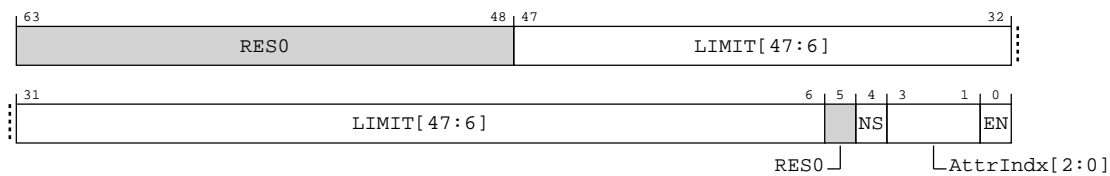


Table A-186: PRLAR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:6]	LIMIT[47:6]	Bits[47:6] of the upper inclusive limit of the selected EL1 MPU memory region. This value is concatenated with the value 0x3F to provide the limit address to be checked against.	42 {x}
[5]	RES0	Reserved	RES0
[4]	NS	Non-secure bit. Specifies whether the output address is in the Secure or Non-secure memory.  <b>0b0</b> Output address is in Secure address space.  <b>0b1</b> Output address is in Non-secure address space.	x
[3:1]	AttrIdx[2:0]	Selects attributes from within the associated Memory Attribute Indirection Register.  <b>0b000</b> Select the Attr0 field from MAIR_EL1.  <b>0b001</b> Select the Attr1 field from MAIR_EL1.  <b>0b010</b> Select the Attr2 field from MAIR_EL1.  <b>0b011</b> Select the Attr3 field from MAIR_EL1.  <b>0b100</b> Select the Attr4 field from MAIR_EL1.  <b>0b101</b> Select the Attr5 field from MAIR_EL1.  <b>0b110</b> Select the Attr6 field from MAIR_EL1.  <b>0b111</b> Select the Attr7 field from MAIR_EL1.	xxx
[0]	EN	Region enable bit.  <b>0b0</b> Region disabled.  <b>0b1</b> Region enabled.	0b0

## Access

Any access to MPU region register PRLAR<n>\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRLAR<n>\_EL1 return an **UNKNOWN** value.
- Writes to unimplemented PRLAR<n>\_EL1 register make all PRLAR\_EL1 registers value **UNKNOWN**.

MRS <Xt>, PRLAR<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	'1':m[3:1]	m[0]:'01'

MSR PRLAR<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	'1':m[3:1]	m[0]:'01'

## Accessibility

Any access to MPU region register PRLAR<n>\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRLAR<n>\_EL1 return an UNKNOWN value.
- Writes to unimplemented PRLAR<n>\_EL1 register make all PRLAR\_EL1 registers value UNKNOWN.

MRS <Xt>, PRLAR<m>\_EL1

```
integer m = UInt(CRm<2:0>:op2<2>);
if (UInt(PRSELR_EL1.REGION<7:4>) * 16) + m >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        X[t, 64] = PRLAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)];
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRLAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)];
```

MSR PRLAR<m>\_EL1, <Xt>

```
integer m = UInt(CRm<2:0>:op2<2>);
if (UInt(PRSELR_EL1.REGION<7:4>) * 16) + m >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        PRLAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)] = X[t, 64];
elseif PSTATE.EL == EL2 then
    PRLAR_EL1[m + (UInt(AArch64-PRSELR_EL1.REGION<7:4>) * 16)] = X[t, 64];
```



A.2.2.27 FAR\_EL1, Fault Address Register (EL1)

Holds the faulting Virtual Address for all synchronous Instruction Abort exceptions, Data Abort exceptions, PC alignment fault exceptions and Watchpoint exceptions that are taken to EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

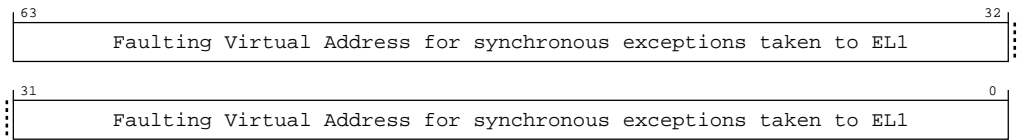
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-75: AARCH64\_FAR\_EL1 bit assignments



**Table A-189: FAR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	None	<p>Faulting Virtual Address for synchronous exceptions taken to EL1. Exceptions that set the FAR_EL1 are Instruction Aborts (EC 0x20 or 0x21), Data Aborts (EC 0x24 or 0x25), PC alignment faults (EC 0x22), and Watchpoints (EC 0x34 or 0x35). AArch64-ESR_EL1.EC holds the EC value for the exception.</p> <p>For a synchronous External abort, if the VA that generated the abort was from an address range for which TCR_ELx.TBI{&lt;0 1&gt;} == 1 for the translation regime in use when the abort was generated, then the top eight bits of FAR_EL1 are <b>UNKNOWN</b>.</p> <p>For a synchronous External abort other than a synchronous External abort on a translation table walk, this field is valid only if AArch64-ESR_EL1.FnV is 0, and FAR_EL1 is <b>UNKNOWN</b> if AArch64-ESR_EL1.FnV is 1.</p> <p>If a memory fault that sets FAR_EL1, other than a Tag Check Fault, is generated from a data cache maintenance or other DC instruction, this field holds the address specified in the register argument of the instruction.</p> <p>For a Data Abort exception or Watchpoint exception, if address tagging is enabled for the address accessed by the data access that caused the exception, then this field includes the tag. For more information about address tagging, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>Execution at EL0 makes FAR_EL1 become <b>UNKNOWN</b>.</p> <p><b>Note:</b> The address held in this field is an address accessed by the instruction fetch or data access that caused the exception that actually gave rise to the instruction or data abort. It is the lower address that gave rise to the fault that is reported. Where different faults from different addresses arise from the same instruction, such as for an instruction that loads or stores an unaligned address that crosses a page boundary, the architecture does not prioritize which fault is reported.</p> <p>For all other exceptions taken to EL1, FAR_EL1 is <b>UNKNOWN</b>.</p> <p>FAR_EL1 is made <b>UNKNOWN</b> on an exception return from EL1.</p>	64 {x}

## Access

MRS &lt;Xt&gt;, FAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0000	0b000

MSR FAR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0000	0b000

## Accessibility

MRS &lt;Xt&gt;, FAR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    
```

```
    else
        X[t, 64] = FAR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = FAR_EL1;
```

MSR FAR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        FAR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    FAR_EL1 = X[t, 64];
```

A.2.2.28 PRENR\_EL1, Protection Region Enable Register (EL1)

Provides direct access to the AArch64-PRLAR\_EL1.EN bits of EL1 MPU regions from 0 to 31.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-76: AARCH64\_PRENR\_EL1 bit assignments

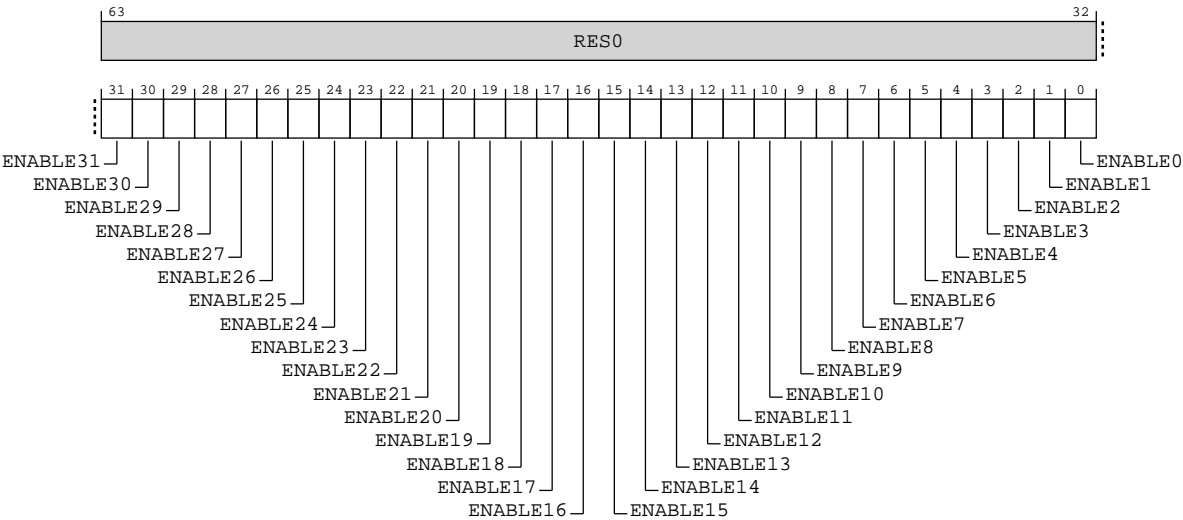


Table A-192: PRENR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	ENABLE<n>, bit[n], where n = 31 to 0	Enable bit. Each bit, n, enables or disables the respective EL1 MPU region. The bits associated with the unimplemented MPU regions are <b>RAZ/WI</b> .  <b>0b0</b> Disables the EL1 MPU n region.  <b>0b1</b> Enables the EL1 MPU n region.	0x00000000

Access

MRS <Xt>, PRENR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0001	0b001

MSR PRENR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0001	0b001

Accessibility

MRS <Xt>, PRENR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TVM == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
elsif VTCR_EL2.MSA == '1' then
    UNDEFINED;
else
    X[t, 64] = PRENR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = PRENR_EL1;
```

MSR PRENR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        PRENR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    PRENR_EL1 = X[t, 64];
```

A.2.2.29 PRSELR\_EL1, Protection Region Selection Register (EL1)

Selects the region number for the EL1 MPU region associated with the AArch64-PRBAR\_EL1 and AArch64-PRLAR\_EL1 registers.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-77: AARCH64\_PRSELR\_EL1 bit assignments

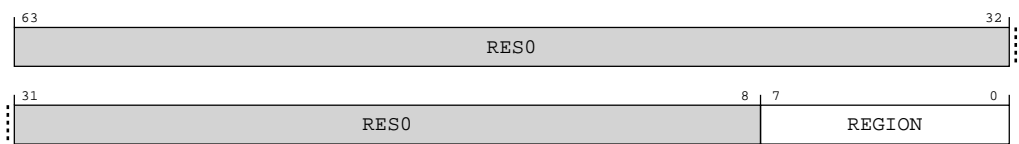


Table A-195: PRSELR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	REGION	The number of the current EL1 MPU region visible in AArch64-PRBAR_EL1 and AArch64-PRLAR_EL1. For N implemented MPU regions, memory region numbering starts at 0 and increments by 1 to the value N-1.  Writing a value greater than or equal to the number of implemented MPU regions specified by AArch64-MPUIR_EL1.REGION, results in CONSTRAINED UNPREDICTABLE behavior.  CONSTRAINED UNPREDICTABLE behavior is that PRSELR_EL1 register becomes <b>UNKNOWN</b> .	8{x}

Access

MRS <Xt>, PRSELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0010	0b001

MSR PRSELR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b0010	0b001

Accessibility

MRS <Xt>, PRSELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        X[t, 64] = PRSELR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRSELR_EL1;
```

MSR PRSELR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
  if HCR_EL2.TVM == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  elseif VTCR_EL2.MSA == '1' then
    UNDEFINED;
  else
    PRSELR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
  PRSELR_EL1 = X[t, 64];
```

A.2.2.30 PRBAR\_EL1, Protection Region Base Address Register (EL1)

Provides access to the base addresses for the EL1 MPU region. AArch64-PRSELR\_EL1.REGION determines which MPU region is selected.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

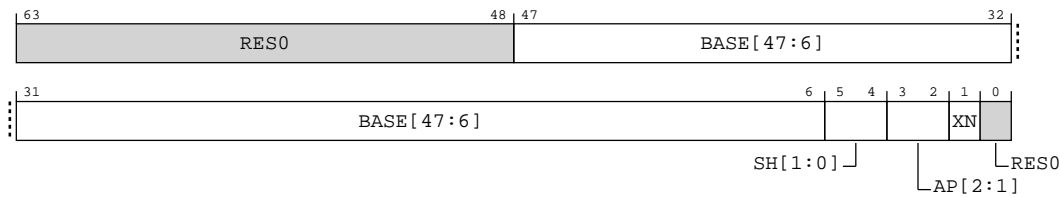


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-78: AARCH64\_PRBAR\_EL1 bit assignments



**Table A-198: PRBAR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	BASE[47:6]	Bits[47:6] of the lower inclusive limit of the selected EL1 MPU memory region. This value is zero extended to provide the base address to be checked against.	42 {x}
[5:4]	SH[1:0]	Shareability attribute.  <b>0b00</b> Non-shareable  <b>0b01</b> Reserved, <b>CONSTRAINED UNPREDICTABLE</b>  <b>0b10</b> Outer Shareable  <b>0b11</b> Inner Shareable	xx
[3:2]	AP[2:1]	Access Permission attributes.  <b>0b00</b> Read/write at EL1, no access at EL0  <b>0b01</b> Read/write at EL1 and EL0  <b>0b10</b> Read-only at EL1, no access at EL0  <b>0b11</b> Read-only at EL1 and EL0	xx
[1]	XN	Execute Never  <b>0b0</b> Execution of instructions fetched from the region is permitted.  <b>0b1</b> Execution of instructions fetched from the region is not permitted.	x
[0]	RES0	Reserved	RES0

## Access

Any access to MPU region register PRBAR\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRBAR\_EL1 register return an **UNKNOWN** value.
- Writes to unimplemented PRBAR\_EL1 register make all PRBAR\_EL1 registers value **UNKNOWN**.

MRS <Xt>, PRBAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b1000	0b000

MSR PRBAR\_EL1, <Xt>



op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b1000	0b000

### Accessibility

Any access to MPU region register PRBAR\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRBAR\_EL1 register return an UNKNOWN value.
- Writes to unimplemented PRBAR\_EL1 register make all PRBAR\_EL1 registers value UNKNOWN.

MRS <Xt>, PRBAR\_EL1

```
if UInt(PRSEL_EL1.REGION) >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        X[t, 64] = PRBAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)];
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRBAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)];
```

MSR PRBAR\_EL1, <Xt>

```
if UInt(PRSEL_EL1.REGION) >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        PRBAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)] = X[t, 64];
elseif PSTATE.EL == EL2 then
    PRBAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)] = X[t, 64];
```

### A.2.2.31 PRLAR\_EL1, Protection Region Limit Address Register (EL1)

Provides access to the limit addresses for the EL1 MPU region. AArch64-PRSEL\_EL1.REGION determines which MPU region is selected.

### Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-79: AARCH64\_PRLAR\_EL1 bit assignments

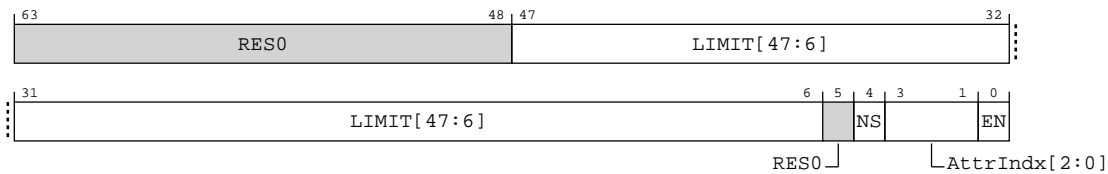


Table A-201: PRLAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	LIMIT[47:6]	Bits[47:6] of the upper inclusive limit of the selected EL1 MPU memory region. This value is concatenated with the value 0x3F to provide the limit address to be checked against.	42 {x}
[5]	RES0	Reserved	RES0
[4]	NS	Non-secure bit. Specifies whether the output address is in the Secure or Non-secure memory.  <b>0b0</b> Output address is in Secure address space.  <b>0b1</b> Output address is in Non-secure address space.	x

Bits	Name	Description	Reset
[3:1]	AttrIndx[2:0]	<p>Selects attributes from within the associated Memory Attribute Indirection Register.</p> <p><b>0b000</b> Select the Attr0 field from MAIR_EL1.</p> <p><b>0b001</b> Select the Attr1 field from MAIR_EL1.</p> <p><b>0b010</b> Select the Attr2 field from MAIR_EL1.</p> <p><b>0b011</b> Select the Attr3 field from MAIR_EL1.</p> <p><b>0b100</b> Select the Attr4 field from MAIR_EL1.</p> <p><b>0b101</b> Select the Attr5 field from MAIR_EL1.</p> <p><b>0b110</b> Select the Attr6 field from MAIR_EL1.</p> <p><b>0b111</b> Select the Attr7 field from MAIR_EL1.</p>	xxx
[0]	EN	<p>Region enable bit.</p> <p><b>0b0</b> Region disabled.</p> <p><b>0b1</b> Region enabled.</p>	0b0

## Access

Any access to MPU region register PRLAR\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRLAR\_EL1 register return an **UNKNOWN** value.
- Writes to unimplemented PRLAR\_EL1 register make all PRLAR\_EL1 registers value **UNKNOWN**.

MRS <Xt>, PRLAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b1000	0b001

MSR PRLAR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0110	0b1000	0b001

## Accessibility

Any access to MPU region register PRLAR\_EL1 above the number of implemented regions specified by AArch64-MPUIR\_EL1.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRLAR\_EL1 register return an UNKNOWN value.
- Writes to unimplemented PRLAR\_EL1 register make all PRLAR\_EL1 registers value UNKNOWN.

MRS <Xt>, PRLAR\_EL1

```

if UInt(PRSEL_EL1.REGION) >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        X[t, 64] = PRLAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)];
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRLAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)];

```

MSR PRLAR\_EL1, <Xt>

```

if UInt(PRSEL_EL1.REGION) >= UInt(MPUIR_EL1.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif VTCR_EL2.MSA == '1' then
        UNDEFINED;
    else
        PRLAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)] = X[t, 64];
elseif PSTATE.EL == EL2 then
    PRLAR_EL1[UInt(AArch64-PRSEL_EL1.REGION)] = X[t, 64];

```

### A.2.2.32 PAR\_EL1, Physical Address Register

Returns the output address (OA) from an Address translation instruction that executed successfully, or fault information if the instruction did not execute successfully.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

When AArch64-PAR\_EL1.F == '0'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-PAR\_EL1.F == '1'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When AArch64-PAR\_EL1.F == '0'

This section describes the register value returned by the successful execution of an Address translation instruction. Software might subsequently write a different value to the register, and that write does not affect the operation of the PE.

On a successful conversion, the PAR\_EL1 can return a value that indicates the resulting attributes, rather than the values that appear in the translation table descriptors. More precisely:

- The PAR\_EL1.{ATTR, SH} fields are permitted to report the resulting attributes, instead of reporting the values that appear in the translation table descriptors.
- See the PAR\_EL1.NS bit description for constraints on the value it returns.

Figure A-80: AARCH64\_PAR\_EL1 bit assignments

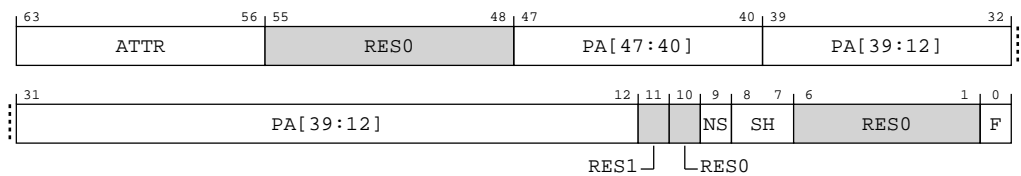


Table A-204: PAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:56]	ATTR	Memory attributes for the returned output address. This field uses the same encoding as the Attr<n> fields in AArch64-MAIR_EL1 and AArch64-MAIR_EL2.  The value returned in this field can be the resulting attribute, instead of the value that appears in the translation table descriptor.	8 {x}

Bits	Name	Description	Reset
[55:48]	<b>RES0</b>	Reserved	<b>RES0</b>
[47:40]	PA[47:40]	<p><b>When PA_W == 48</b></p> <p>Output address. The output address (OA) corresponding to the supplied input address. This field returns address bits[47:40].</p> <p><b>Otherwise</b></p> <p>RES0</p>	8 {x}
[39:12]	PA[39:12]	Output address. The output address (OA) corresponding to the supplied input address. This field returns address bits[39:12].	28 {x}
[11]	<b>RES1</b>	Reserved	<b>RES1</b>
[10]	<b>RES0</b>	Reserved	<b>RES0</b>
[9]	NS	<p>Non-secure. The NS attribute for a translation table entry from a Secure translation regime.</p> <p>This bit reflects the Security state of the intermediate physical address space of the translation for the instructions:</p> <ul style="list-style-type: none"> <li>AT S1E1R, AT S1E1W, AT S1E1RP, AT S1E1WP, AT S1E0R, and AT S1E0W.</li> </ul> <p>Otherwise, this bit reflects the Security state of the physical address space of the translation. This means it reflects the effect of the NSTable bits of earlier levels of the translation table walk if those NSTable bits have an effect on the translation.</p>	x
[8:7]	SH	<p>Shareability attribute, for the returned output address. Permitted values are:</p> <p><b>0b00</b></p> <p>Non-shareable.</p> <p><b>0b10</b></p> <p>Outer Shareable.</p> <p><b>0b11</b></p> <p>Inner Shareable.</p> <p>The value 0b01 is reserved.</p> <p><b>Note:</b></p> <p>This field returns the value 0b10 for:</p> <ul style="list-style-type: none"> <li>Any type of Device memory.</li> <li>Normal memory with both Inner Non-cacheable and Outer Non-cacheable attributes.</li> </ul> <p>The value returned in this field can be the resulting attribute, instead of the value that appears in the translation table descriptor.</p>	xx
[6:1]	<b>RES0</b>	Reserved	<b>RES0</b>
[0]	F	<p>Indicates whether the instruction performed a successful address translation.</p> <p><b>0b0</b></p> <p>Address translation completed successfully.</p>	x

When AArch64-PAR\_EL1.F == '1'

This section describes the register value returned by a fault on the execution of an Address translation instruction. Software might subsequently write a different value to the register, and that write does not affect the operation of the PE.

Figure A-81: AARCH64\_PAR\_EL1 bit assignments

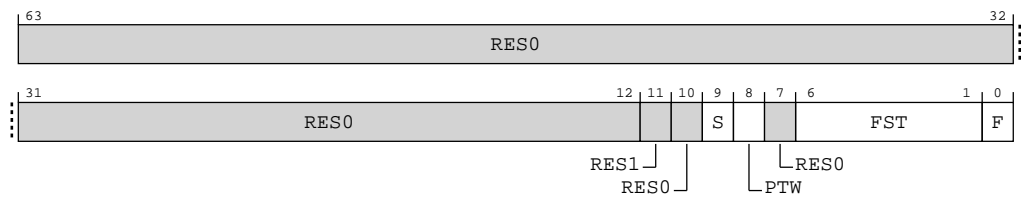


Table A-205: PAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:12]	RES0	Reserved	RES0
[11]	RES1	Reserved	RES1
[10]	RES0	Reserved	RES0
[9]	S	Indicates the translation stage at which the translation aborted:  <b>0b0</b> Translation aborted because of a fault in the stage 1 translation.  <b>0b1</b> Translation aborted because of a fault in the stage 2 translation.	x
[8]	PTW	If this bit is set to 1, it indicates the translation aborted because of a stage 2 fault during a stage 1 translation table walk.	x
[7]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[6:1]	FST	<p>Fault status code, as shown in the Data Abort ESR encoding.</p> <p><b>0b000000</b> Address size fault, level 0 of translation or translation table base register.</p> <p><b>0b000001</b> Address size fault, level 1.</p> <p><b>0b000010</b> Address size fault, level 2.</p> <p><b>0b000011</b> Address size fault, level 3.</p> <p><b>0b000100</b> Translation fault, level 0.</p> <p><b>0b000101</b> Translation fault, level 1.</p> <p><b>0b000110</b> Translation fault, level 2.</p> <p><b>0b000111</b> Translation fault, level 3.</p> <p><b>0b001001</b> Access flag fault, level 1.</p> <p><b>0b001010</b> Access flag fault, level 2.</p> <p><b>0b001011</b> Access flag fault, level 3.</p> <p><b>0b001100</b> Permission fault, level 0.</p> <p><b>0b001101</b> Permission fault, level 1.</p> <p><b>0b001110</b> Permission fault, level 2.</p> <p><b>0b001111</b> Permission fault, level 3.</p> <p><b>0b010100</b> Synchronous External abort on translation table walk or hardware update of translation table, level 0.</p> <p><b>0b010101</b> Synchronous External abort on translation table walk or hardware update of translation table, level 1.</p> <p><b>0b010110</b> Synchronous External abort on translation table walk or hardware update of translation table, level 2.</p> <p><b>0b010111</b> Synchronous External abort on translation table walk or hardware update of translation table, level 3.</p> <p><b>0b110000</b> TLB conflict abort.</p> <p><b>0b110001</b> Unsupported atomic hardware update fault.</p>	6 {x}



Bits	Name	Description	Reset
[0]	F	Indicates whether the instruction performed a successful address translation.  <b>0b1</b> Address translation aborted.	x

**Access**  
MRS <Xt>, PAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0111	0b0100	0b000

MSR PAR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0111	0b0100	0b000

**Accessibility**  
MRS <Xt>, PAR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = PAR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PAR_EL1;
```

MSR PAR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    PAR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    PAR_EL1 = X[t, 64];
```

A.2.2.33 MAIR\_EL1, Memory Attribute Indirection Register (EL1)

If VM8-64 is enabled at stage 1 of EL1&0 translation regime, this register provides the memory attribute encodings corresponding to the possible AttrIdx values in a Long-descriptor format translation table entry for stage 1 translations at EL1.

If PM8-64 is enabled at stage 1 of EL1&0 translation regime, this register provides the memory attribute encodings corresponding to the possible AttrIdx values in AArch64-PRLAR\_EL1 register for stage 1 translations.

**Configurations**  
This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

MAIR\_EL1 is permitted to be cached in a TLB.

Figure A-82: AARCH64\_MAIR\_EL1 bit assignments

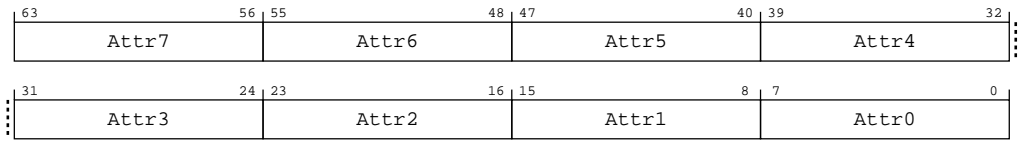


Table A-208: MAIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	Attr<n>	<p>The memory attribute encoding for an AttrIdx[2:0] gives the value of &lt;n&gt; in Attr&lt;n&gt;.</p> <p>Attr is encoded as follows: <a href="#">Table A-209: Attr description</a> on page 519</p> <p>'dd' is encoded as follows: <a href="#">Table A-210: dd description</a> on page 519</p> <p>'oooo' is encoded as follows: <a href="#">Table A-211: 'oooo' description</a> on page 519</p> <p>R = Outer Read-Allocate policy, W = Outer Write-Allocate policy.</p> <p>'iiii' is encoded as follows: <a href="#">Table A-212: 'iiii' description</a> on page 519</p> <p>R = Inner Read-Allocate policy, W = Inner Write-Allocate policy.</p> <p>The R and W bits in 'oooo' and 'iiii' fields have the following meanings: <a href="#">Table A-213: R or W description</a> on page 519</p>	64 {x}

**Table A-209: Attr description**

Attr	Meaning
0b0000dd00	Device memory. See encoding of 'dd' for the type of Device memory.
0b0000ddxx, (xx != 00)	UNPREDICTABLE.
0booooiiii, (oooo != 0000 and iiii != 0000)	Normal memory. See encoding of 'oooo' and 'iiii' for the type of Normal Memory.
0bxxxx0000, where xxxx != 0000	UNPREDICTABLE.

**Table A-210: dd description**

dd	Meaning
0b00	Device-nGnRnE memory
0b01	Device-nGnRE memory
0b10	Device-nGRE memory
0b11	Device-GRE memory

**Table A-211: 'oooo' description**

'oooo'	Meaning
0b0000	See encoding of Attr
0b00RW, RW not 0b00	Normal memory, Outer Write-Through Transient
0b0100	Normal memory, Outer Non-cacheable
0b01RW, RW not 0b00	Normal memory, Outer Write-Back Transient
0b10RW	Normal memory, Outer Write-Through Non-transient
0b11RW	Normal memory, Outer Write-Back Non-transient

**Table A-212: 'iiii' description**

'iiii'	Meaning
0b0000	See encoding of Attr
0b00RW, RW not 0b00	Normal memory, Inner Write-Through Transient
0b0100	Normal memory, Inner Non-cacheable
0b01RW, RW not 0b00	Normal memory, Inner Write-Back Transient
0b10RW	Normal memory, Inner Write-Through Non-transient
0b11RW	Normal memory, Inner Write-Back Non-transient

**Table A-213: R or W description**

R or W	Meaning
0b0	No Allocate
0b1	Allocate

## Access

MRS &lt;Xt&gt;, MAIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0010	0b000

MSR MAIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0010	0b000

Accessibility

MRS <Xt>, MAIR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MAIR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MAIR_EL1;
```

MSR MAIR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        MAIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    MAIR_EL1 = X[t, 64];
```

A.2.2.34 AMAIR\_EL1, Auxiliary Memory Attribute Indirection Register (EL1)

Provides **IMPLEMENTATION DEFINED** memory attributes for the memory regions specified by AArch64-MAIR\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

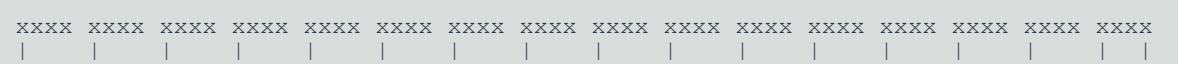
Functional group

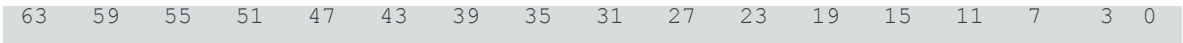
Generic System Control

Access type

See bit descriptions

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-83: AARCH64\_AMAIR\_EL1 bit assignments

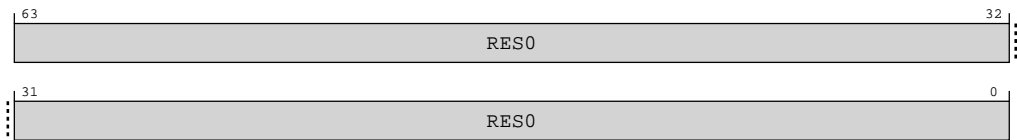


Table A-216: AMAIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, AMAIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0011	0b000

MSR AMAIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0011	0b000

Accessibility

MRS <Xt>, AMAIR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = AMAIR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = AMAIR_EL1;
```

MSR AMAIR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
  if HCR_EL2.TVM == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    AMAIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
  AMAIR_EL1 = X[t, 64];
```

A.2.2.35 VBAR\_EL1, Vector Base Address Register (EL1)

Holds the vector base address for any exception that is taken to EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

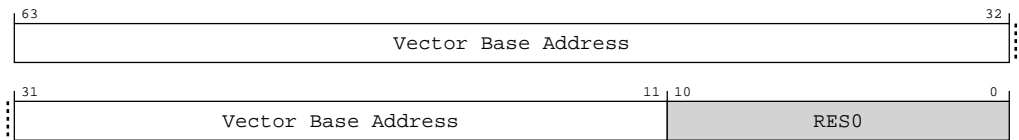
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-84: AARCH64\_VBAR\_EL1 bit assignments



**Table A-219: VBAR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:11]	None	Vector Base Address. Base address of the exception vectors for exceptions taken to EL1.  <b>Note:</b> <ul style="list-style-type: none"> <li>If tagged addresses are being used, bits [55:48] of VBAR_EL1 must be the same or else the use of the vector address will result in a recursive exception.</li> <li>If tagged addresses are not being used, bits [63:48] of VBAR_EL1 must be the same or else the use of the vector address will result in a recursive exception.</li> </ul>	53 {x}
[10:0]	RES0	Reserved	RES0

### Access

MRS &lt;Xt&gt;, VBAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0000	0b000

MSR VBAR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0000	0b000

### Accessibility

MRS &lt;Xt&gt;, VBAR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = VBAR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VBAR_EL1;

```

MSR VBAR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    VBAR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    VBAR_EL1 = X[t, 64];

```

### A.2.2.36 ISR\_EL1, Interrupt Status Register

Shows the pending status of the IRQ, FIQ, or SError interrupt.

When executing at EL2, this shows the pending status of the physical IRQ, FIQ, or SError interrupts.

When executing at EL1:

- If the AArch64-HCR\_EL2.{IMO,FMO,AMO} bit has a value of 1, the corresponding ISR\_EL1.{I,F,A} bit shows the pending status of the virtual IRQ, FIQ, or SError.
- If the AArch64-HCR\_EL2.{IMO,FMO,AMO} bit has a value of 0, the corresponding ISR\_EL1.{I,F,A} bit shows the pending status of the physical IRQ, FIQ, or SError.

Configurations

This register is available in all configurations.

Attributes

Width

64

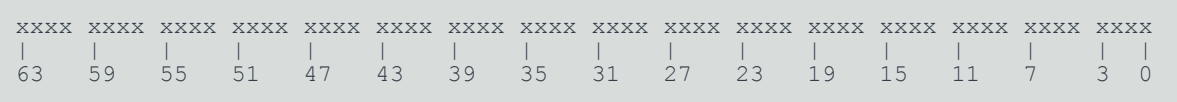
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-85: AARCH64\_ISR\_EL1 bit assignments

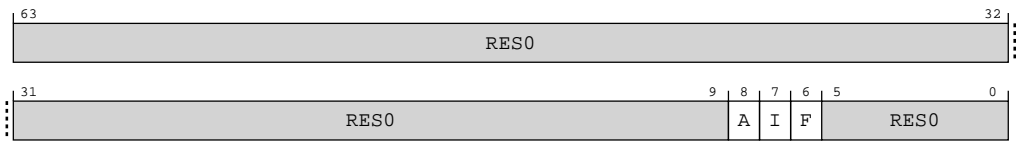


Table A-222: ISR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:9]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[8]	A	SError interrupt pending bit. Indicates whether an SError interrupt is pending.  <b>0b0</b> No pending SError.  <b>0b1</b> An SError interrupt is pending.  If the SError interrupt is edge-triggered, this field is cleared to zero when the physical SError interrupt is taken.	x
[7]	I	IRQ pending bit. Indicates whether an IRQ interrupt is pending.  <b>0b0</b> No pending IRQ.  <b>0b1</b> An IRQ interrupt is pending.  <b>Note:</b> This bit indicates the presence of a pending IRQ interrupt regardless of whether the interrupt has Superpriority.	x
[6]	F	FIQ pending bit. Indicates whether an FIQ interrupt is pending.  <b>0b0</b> No pending FIQ.  <b>0b1</b> An FIQ interrupt is pending.  <b>Note:</b> This bit indicates the presence of a pending FIQ interrupt regardless of whether the interrupt has Superpriority.	x
[5:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ISR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0001	0b000

Accessibility

MRS <Xt>, ISR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    X[t, 64] = ISR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ISR_EL1;
```

A.2.2.37 CONTEXTIDR\_EL1, Context ID Register (EL1)

Identifies the current Process Identifier.

The value of the whole of this register is called the Context ID and is used by:

- The debug logic, for Linked and Unlinked Context ID matching.
- The trace logic, to identify the current process.

The significance of this register is for debug and trace use only.

Configurations

This register is available in all configurations.

Attributes

Width

64

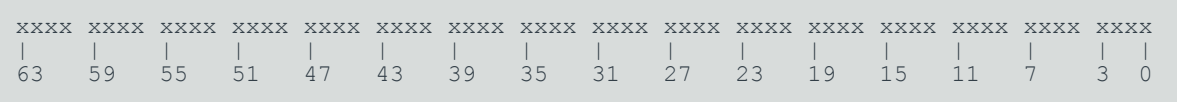
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-86: AARCH64\_CONTEXTIDR\_EL1 bit assignments

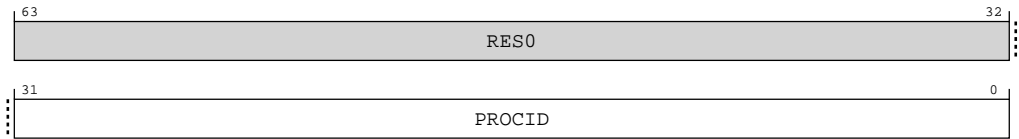


Table A-224: CONTEXTIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:0]	PROCID	Process Identifier. This field must be programmed with a unique value that identifies the current process.  <b>Note:</b> In AArch64 state, CONTEXTIDR_EL1 is independent of the ASID, and for the EL1&0 translation regime either AArch64-TTBRO_EL1 or AArch64-TTBR1_EL1 holds the ASID.	32 {x}

### Access

MRS <Xt>, CONTEXTIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1101	0b0000	0b001

MSR CONTEXTIDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1101	0b0000	0b001

### Accessibility

MRS <Xt>, CONTEXTIDR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = CONTEXTIDR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = CONTEXTIDR_EL1;

```

MSR CONTEXTIDR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        CONTEXTIDR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
        CONTEXTIDR_EL1 = X[t, 64];

```

## A.2.2.38 TPIDR\_EL1, EL1 Software Thread ID Register

Provides a location where software executing at EL1 can store thread identifying information, for OS management purposes.

The PE makes no use of this register.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-87: AARCH64\_TPIDR\_EL1 bit assignments

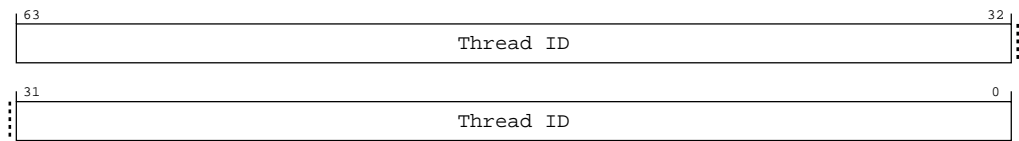


Table A-227: TPIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Thread ID. Thread identifying information stored by software running at this Exception level.	64 {x}

Access

MRS <Xt>, TPIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1101	0b0000	0b100

MSR TPIDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1101	0b0000	0b100

Accessibility

MRS <Xt>, TPIDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    X[t, 64] = TPIDR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = TPIDR_EL1;
```

MSR TPIDR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    TPIDR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    TPIDR_EL1 = X[t, 64];
```

A.2.2.39 IMP\_ITCMREGIONR\_EL1, ITCM Region Register

This register controls the ITCM region.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

inconsistent

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-88: AARCH64\_IMP\_ITCMREGIONR\_EL1 bit assignments

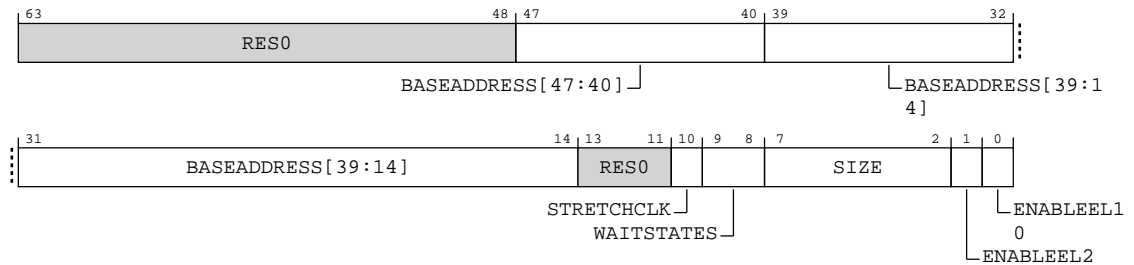


Table A-230: IMP\_ITCMREGIONR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:40]	BASEADDRESS[47:40]	<b>When PA_W == 48</b> TCM base address, bits [47:40]. This field is read-only. This field takes the value of the CFGITCMBASEADDRm[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:14]	BASEADDRESS[39:14]	TCM base address, bits [39:14] (aligned to TCM size). This field is read-only. This field takes the value of the CFGITCMBASEADDRm[39:14] configuration pins.  Access to this field is: RO	26 {x}
[13:11]	RES0	Reserved	RES0
[10]	STRETCHCLK	TCM clock stretch. This field is read-only. This field takes the value of the ITCM_STRETCH_CLKm core parameter.  <b>0b0</b> No clock stretch.  <b>0b1</b> Clock stretched to occupy full cycle.  Access to this field is: RO	x
[9:8]	WAITSTATES	TCM accesses wait states: 0-3 cycles. This field is read-only. This field takes the value of the ITCM_WAITm core parameter.  Access to this field is: RO	xx

Bits	Name	Description	Reset
[7:2]	SIZE	<p>TCM size, encoded as <math>1 + \log_2(\text{size}/1\text{KB})</math>. This field is read-only. This field takes the value of the ITCM_SIZE<sub>m</sub> core parameter.</p> <p><b>0b000000</b> no TCM present.</p> <p><b>0b000101</b> 16 KB.</p> <p><b>0b000110</b> 32 KB.</p> <p><b>0b000111</b> 64 KB.</p> <p><b>0b001000</b> 128 KB.</p> <p><b>0b001001</b> 256 KB.</p> <p><b>0b001010</b> 512 KB.</p> <p><b>0b001011</b> 1 MB.</p> <p>Access to this field is: RO</p>	6 {x}
[1]	ENABLEEL2	<p>TCM enable at EL2. This field is read-only in EL1 or EL0. This field resets to the value of the CFGITCMEN<sub>m</sub> configuration pin.</p> <p><b>0b0</b> TCM disabled at EL2.</p> <p><b>0b1</b> TCM enabled at EL2.</p> <p><b>When PSTATE.EL == EL2</b> Access to this field is: RW</p> <p><b>Otherwise</b> Access to this field is: RO</p>	x
[0]	ENABLEEL10	<p>TCM enable at EL1 and EL0. If the stage 1 EL1&amp;0 translation regime uses the VMSAv8-64 memory architecture, this field reads and behaves as 0 and ignores writes.</p> <p><b>0b0</b> TCM disabled at EL1 and EL0.</p> <p><b>0b1</b> TCM enabled at EL1 and EL0.</p> <p><b>When PSTATE.EL == EL2 or AArch64-VTCR_EL2.MSA == '0'</b> Access to this field is: RW</p> <p><b>Otherwise</b> Access to this field is: RAZ/WI</p>	0b0

Access

MRS <Xt>, IMP\_ITCMREGIONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b001

MSR IMP\_ITCMREGIONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b001

Accessibility

MRS <Xt>, IMP\_ITCMREGIONR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_ITCMREGIONR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_ITCMREGIONR_EL1;
```

MSR IMP\_ITCMREGIONR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.REGIONS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_ITCMREGIONR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_ITCMREGIONR_EL1 = X[t, 64];
```

A.2.2.40 IMP\_DTCMREGIONR\_EL1, DTCM Region Register

This register controls the DTCM region.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control



**Access type**

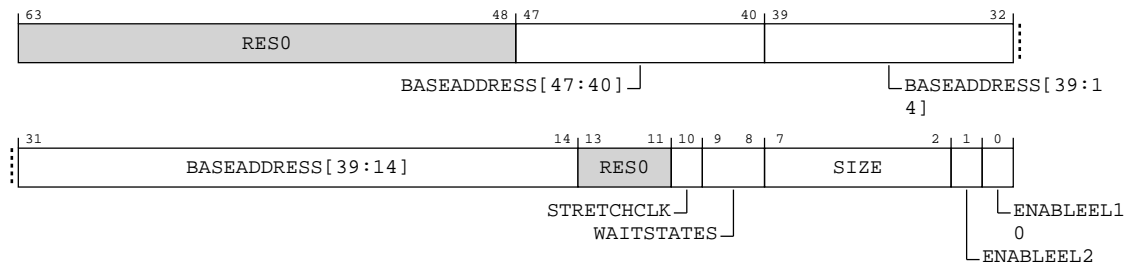
inconsistent

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

**Note**

Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-89: AARCH64\_IMP\_DTCMREGIONR\_EL1 bit assignments****Table A-233: IMP\_DTCMREGIONR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:40]	BASEADDRESS[47:40]	<b>When PA_W == 48</b> TCM base address, bits [47:40]. This field is read-only. This field takes the value of the CFGDTCMBASEADDRm[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:14]	BASEADDRESS[39:14]	TCM base address, bits [39:14] (aligned to TCM size). This field is read-only. This field takes the value of the CFGDTCMBASEADDRm[39:14] configuration pins.  Access to this field is: RO	26 {x}
[13:11]	RES0	Reserved	RES0
[10]	STRETCHCLK	TCM clock stretch. This field is read-only. This field takes the value of the DTCM_STRETCH_CLKm core parameter.  <b>0b0</b> No clock stretch.  <b>0b1</b> Clock stretched to occupy full cycle.  Access to this field is: RO	x

Bits	Name	Description	Reset
[9:8]	WAITSTATES	TCM accesses wait states: 0-3 cycles. This field is read-only. This field takes the value of the DTCM_WAITm core parameter.  Access to this field is: RO	xx
[7:2]	SIZE	TCM size, encoded as $1 + \log_2(\text{size}/1\text{KB})$ . This field is read-only. This field takes the value of the DTCM_SIZEEm core parameter.  <b>0b000000</b> no TCM present.  <b>0b000101</b> 16 KB.  <b>0b000110</b> 32 KB.  <b>0b000111</b> 64 KB.  <b>0b001000</b> 128 KB.  <b>0b001001</b> 256 KB.  <b>0b001010</b> 512 KB.  <b>0b001011</b> 1 MB.  Access to this field is: RO	6{x}
[1]	ENABLEEL2	TCM enable at EL2. This field is read-only in EL1 or EL0.  <b>0b0</b> TCM disabled at EL2.  <b>0b1</b> TCM enabled at EL2.  <b>When PSTATE.EL == EL2</b> Access to this field is: RW  <b>Otherwise</b> Access to this field is: RO	0b0
[0]	ENABLEEL10	TCM enable at EL1 and EL0. If the stage 1 EL1&0 translation regime uses the VMSAv8-64 memory architecture, this field reads and behaves as 0 and ignores writes.  <b>0b0</b> TCM disabled at EL1 and EL0.  <b>0b1</b> TCM enabled at EL1 and EL0.  <b>When PSTATE.EL == EL2 or AArch64-VTCR_EL2.MSA == '0'</b> Access to this field is: RW  <b>Otherwise</b> Access to this field is: RAZ/WI	0b0

Access

MRS <Xt>, IMP\_DTCMREGIONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b010

MSR IMP\_DTCMREGIONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b010

Accessibility

MRS <Xt>, IMP\_DTCMREGIONR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_DTCMREGIONR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_DTCMREGIONR_EL1;
```

MSR IMP\_DTCMREGIONR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.REGIONS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_DTCMREGIONR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_DTCMREGIONR_EL1 = X[t, 64];
```

A.2.2.41 IMP\_LLPPREGIONR\_EL1, LLPP Region Register

This register controls the LLPP region.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

**Access type**

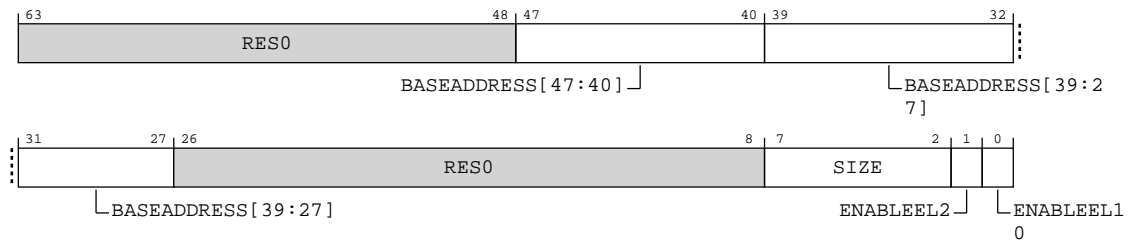
RO

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-90: AARCH64\_IMP\_LLPPREGIONR\_EL1 bit assignments****Table A-236: IMP\_LLPPREGIONR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:40]	BASEADDRESS[47:40]	<b>When PA_W == 48</b> LLPP base address, bits [47:40]. This field is read-only. This field takes the value of the CFGLLPPBASE[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:27]	BASEADDRESS[39:27]	LLPP base address, bits [39:27] (aligned to 128 MB). This field is read-only. This field takes the value of the CFGLLPPBASE[39:27] configuration pins.  Access to this field is: RO	13 {x}
[26:8]	RES0	Reserved	RES0
[7:2]	SIZE	LLPP size, encoded as $1 + \log_2(\text{size}/1\text{KB})$ . This field is read-only.  <b>0b000000</b> no LLPP present (when the CFGLLPPIMP configuration pin is 0x0)  <b>0b010010</b> 128 MB (when the CFGLLPPIMP configuration pin is 0x1)  Access to this field is: RO	6 {x}

Bits	Name	Description	Reset
[1]	ENABLEEL2	<p>LLPP enable at EL2. This field is read-only in EL1 or EL0.</p> <p><b>0b0</b></p> <p>LLPP disabled at EL2.</p> <p><b>0b1</b></p> <p>LLPP enabled at EL2.</p> <p><b>When PSTATE.EL == EL2</b></p> <p>Access to this field is: RW</p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	0b0
[0]	ENABLEEL10	<p>LLPP enable at EL1 and EL0.</p> <p><b>0b0</b></p> <p>LLPP disabled at EL1 and EL0.</p> <p><b>0b1</b></p> <p>LLPP enabled at EL1 and EL0.</p>	0b0

## Access

MRS <Xt>, IMP\_LLPPREGIONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b011

MSR IMP\_LLPPREGIONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b011

## Accessibility

MRS <Xt>, IMP\_LLPPREGIONR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_LLPPREGIONR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_LLPPREGIONR_EL1;

```

MSR IMP\_LLPPREGIONR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.REGIONS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_LLPPREGIONR_EL1 = X[t, 64];

```

```
elseif PSTATE.EL == EL2 then
    IMP_LLPPREGIONR_EL1 = X[t, 64];
```

A.2.2.42 IMP\_LLRAMREGIONR\_EL1, LLRAM Region Register

This register controls the LLRAM region.

Configurations

This register is available in all configurations.

Attributes

Width

64

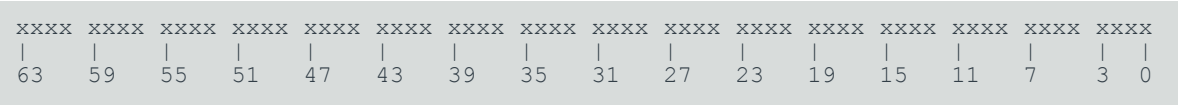
Functional group

Generic System Control

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-91: AARCH64\_IMP\_LLRAMREGIONR\_EL1 bit assignments

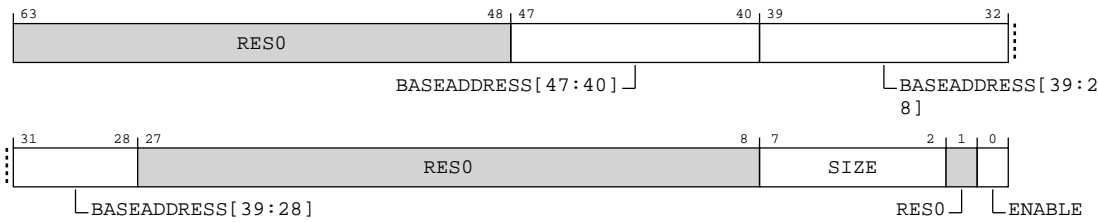


Table A-239: IMP\_LLRAMREGIONR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:40]	BASEADDRESS[47:40]	<b>When PA_W == 48</b> LLRAM base address, bits [47:40]. This field is read-only. This field takes the value of the CFGLLRAMBASE[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:28]	BASEADDRESS[39:28]	LLRAM base address, bits [39:28] (aligned to 256 MB). This field is read-only. This field takes the value of the CFGLLRAMBASE[39:28] configuration pins.  Access to this field is: RO	12 {x}
[27:8]	RES0	Reserved	RES0
[7:2]	SIZE	LLRAM size, encoded as $1 + \log_2(\text{size}/1\text{KB})$ . This field is read-only.  <b>0b000000</b> no LLRAM present (when the CFGLLRAMIMP configuration pin is 0x0)  <b>0b010011</b> 256 MB (when the CFGLLRAMIMP configuration pin is 0x1)  Access to this field is: RO	6 {x}
[1]	RES0	Reserved	RES0
[0]	ENABLE	LLRAM enable. This field resets to the value of the CFGLLRAMEN configuration pin.  <b>Note:</b> This bit controls whether the current core has access to the LLRAM region. It does not enable or disable the LLRAM itself. The LLRAM can be accessed by other cores and can service LLRAM ACP requests regardless of this bit being 0.  <b>0b0</b> LLRAM region disabled.  <b>0b1</b> LLRAM region enabled.	x

## Access

MRS <Xt>, IMP\_LLDRAMREGIONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b100

MSR IMP\_LLDRAMREGIONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b100

## Accessibility

MRS <Xt>, IMP\_LLDRAMREGIONR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_LLRAMREGIONR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_LLRAMREGIONR_EL1;
```

MSR IMP\_LLRAMREGIONR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.REGIONS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_LLRAMREGIONR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_LLRAMREGIONR_EL1 = X[t, 64];
```

A.2.2.43 IMP\_SPPREGIONR\_EL1, SPP Region Register

This register controls the SPP region.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



## Bit descriptions

Figure A-92: AARCH64\_IMP\_SPPREGIONR\_EL1 bit assignments

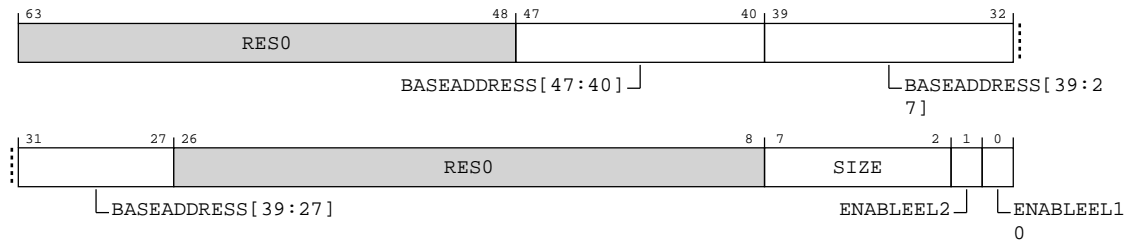


Table A-242: IMP\_SPPREGIONR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:40]	BASEADDRESS[47:40]	<b>When PA_W == 48</b> SPP base address, bits [47:40]. This field is read-only. This field takes the value of the CFGSPPBASE[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:27]	BASEADDRESS[39:27]	SPP base address, bits [39:27] (aligned to 128 MB). This field is read-only. This field takes the value of the CFGSPPBASE[39:27] configuration pins.  Access to this field is: RO	13 {x}
[26:8]	RES0	Reserved	RES0
[7:2]	SIZE	SPP size, encoded as $1 + \log_2(\text{size}/1\text{KB})$ . This field is read-only.  <b>0b000000</b> No SPP present (when the CFGSPPIMP configuration pin is 0x0)  <b>0b010010</b> 128 MB (when the CFGSPPIMP configuration pin is 0x1)  Access to this field is: RO	6 {x}
[1]	ENABLEEL2	SPP enable at EL2. This field is read-only in EL1 or EL0.  <b>Note:</b> This bit controls whether the current core has access to the SPP region from EL2. The SPP can be accessed by other cores from EL2, regardless of this bit being 0.  <b>0b0</b> SPP disabled at EL2.  <b>0b1</b> SPP enabled at EL2.  <b>When PSTATE.EL == EL2</b> Access to this field is: RW  <b>Otherwise</b> Access to this field is: RO	0b0

Bits	Name	Description	Reset
[0]	ENABLEEL10	<p>SPP enable at EL1 and EL0.</p> <p><b>Note:</b> This bit controls whether the current core has access to the SPP region from EL1 and EL0. The SPP can be accessed by other cores from EL1 and EL0, regardless of this bit being 0.</p> <p><b>0b0</b> SPP disabled at EL1 and EL0.</p> <p><b>0b1</b> SPP enabled at EL1 and EL0.</p>	0b0

## Access

MRS <Xt>, IMP\_SPPREGIONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b101

MSR IMP\_SPPREGIONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0000	0b101

## Accessibility

MRS <Xt>, IMP\_SPPREGIONR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_SPPREGIONR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_SPPREGIONR_EL1;

```

MSR IMP\_SPPREGIONR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.REGIONS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_SPPREGIONR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_SPPREGIONR_EL1 = X[t, 64];

```

### A.2.2.44 IMP\_CPUACTLR\_EL1, CPU Auxiliary Control Register

This register contains control bits that affect the CPU behavior.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic System Control

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	x001	0001	0100	1110	1101	0xx0	1111	0011	1000	0111	1111
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-93: AARCH64\_IMP\_CPUACTLR\_EL1 bit assignments

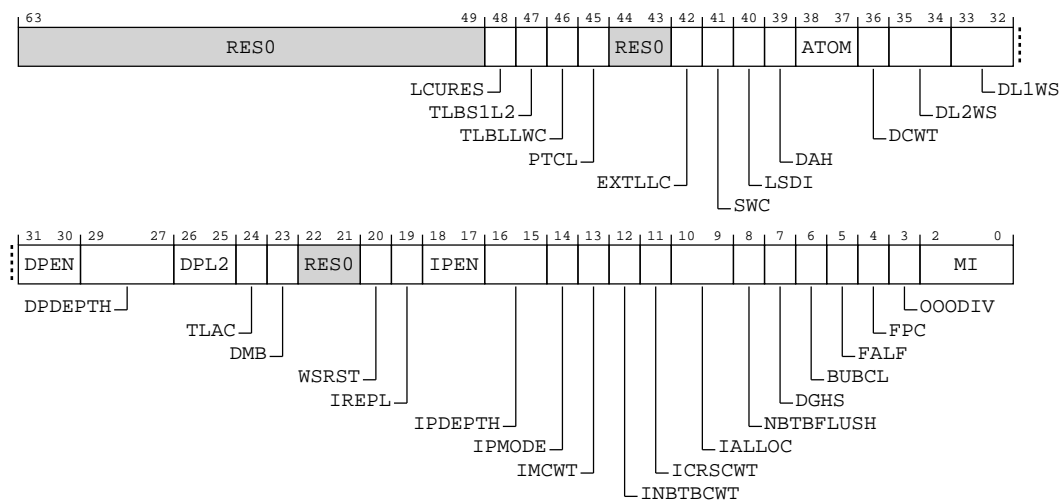


Table A-245: IMP\_CPUACTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:49]	RES0	Reserved	RES0
[48]	LCURES	<p><b>When CFGLLRAMIMP == 1 or CFGSPPIMP == 1</b></p> <p>Reserve some CPU resources for LCU (LLRAM and SPP) accesses.</p> <p><b>0b0</b></p> <p>No specific resources are reserved for LLRAM or SPP accesses.</p> <p><b>0b1</b></p> <p>A certain number of STB slots and I-side and D-side linefill descriptors are reserved to ensure that LLRAM and SPP accesses do not have increased worst case latency caused by Main Manager accesses.</p> <p>When this bit is set to 0, accesses to Main Manager can fill up some resources in the CPU (STB slots and linefill descriptors) and the latency of subsequent LLRAM and SPP accesses may be impacted until older transactions have completed and freed these resources.</p> <p>If the value of AArch64-IMP_INTLATENCY_EL2.LCURES is not 0 then PE behaves as if the value of the AArch64-IMP_CPUACTLR_EL1.LCURES field is 1 for all purposes other than returning the value of a direct read of the field.</p> <p><b>Otherwise</b></p> <p>RES0</p>	'0'
[47]	TLBS1L2	<p><b>When VMSAm == 1</b></p> <p>TLB S1L2 walk caching behavior.</p> <p><b>0b0</b></p> <p>TLB S1L2 walk caching disabled.</p> <p><b>0b1</b></p> <p>TLB S1L2 walk caching enabled.</p> <p><b>Otherwise</b></p> <p>RES0</p>	'1'
[46]	TLBLLWC	<p><b>When VMSAm == 1</b></p> <p>TLB Last Level Walk Caching behavior.</p> <p><b>0b0</b></p> <p>TLB last level walk caching disabled.</p> <p><b>0b1</b></p> <p>TLB last level walk caching enabled.</p> <p><b>Otherwise</b></p> <p>RES0</p>	'1'

Bits	Name	Description	Reset
[45]	PTCL	<b>When VMSAm == 1</b> Page Tables Caching Level. <b>0b0</b> Cache page tables in L1. <b>0b1</b> Cache page tables in L2. <b>Otherwise</b> RES0	'0'
[44:43]	RES0	Reserved	RES0
[42]	EXTLLC	External Last-Level Cache present. Affects the counting of cache-related PMU events. Used to control how the LL_CACHE* PMU events count. <b>0b0</b> The last-level cache is the processor L2. <b>0b1</b> An external Last-level cache is present in the system. If the MM uses CHI, the DataSource field will indicate when data is returned from the external cache.	0b0
[41]	SWC	Store buffer Write streaming Cache lookup behavior. <b>0b0</b> Store buffer skips cache lookups while in write-streaming mode. <b>0b1</b> Store buffer performs cache lookups while in write-streaming mode.	0b0
[40]	LSDI	Load/store dual-issuing control. <b>0b0</b> Dual-issuing of load/store instructions disabled. Only the first memory pipeline will be used. Note that a load or store can still be issued with a non-memory instruction. <b>0b1</b> Dual-issuing of load/store instructions enabled.	0b1
[39]	DAH	Disable Allocation Hints. <b>0b0</b> Normal operation. <b>0b1</b> The Inner Allocation and Transient Allocation hints in the MAIR are ignored. All cacheable accesses are forced to inner read and write allocate. The LDNP and STNP instructions behave the same as the equivalent LDP and STP instructions	0b0

Bits	Name	Description	Reset
[38:37]	ATOM	<p>Atomic instructions execution control. This field defines whether certain cacheable atomic instructions in the Main Manager (MM) are executed near or far.</p> <p>The behavior of the instructions below do not depend on the value of the ATOM field:</p> <ul style="list-style-type: none"> <li>All TCM atomics are executed near.</li> <li>Non-cacheable or Device LLRAM atomics are executed far if CFGLLRAMSHARED=1, otherwise they are executed in the cluster.</li> <li>Cacheable LLRAM atomics are executed far if CFGLLRAMSHARED=1 and the memory location is outer shareable, otherwise they are executed in the cluster.</li> <li>Non-cacheable or Device MM atomics are executed far.</li> <li>Cacheable MM atomics are executed near if BROADCASTOUTERM = 0 or BROADCASTATOMICM = 0.</li> <li>Cacheable MM atomics are executed near if the memory location is non-shareable.</li> <li>Cacheable MM atomics are executed near if the memory location is not aligned to the element size.</li> <li>The MM atomic is executed near if it is a hardware access flag pagetable update.</li> </ul> <p>The behavior of the remaining cacheable MM atomics depends on the value of the ATOM field:</p> <p><b>0b00</b> Atomic instructions are executed near if they hit in the cache in a unique state, or far if they miss or are shared.</p> <p><b>0b01</b> Atomic instructions are executed near.</p> <p><b>0b10</b> Most atomic instructions are executed far.</p> <p><b>0b11</b> Load atomics, including SWP and CAS, are executed near. Store atomics are executed near if they hit in the cache in a unique state, or far if they miss or are shared.</p>	0b00
[36]	DCWT	<p>L1 data cache cache way tracker control.</p> <p><b>0b0</b> Cache way tracker disabled.</p> <p><b>0b1</b> Cache way tracker enabled.</p>	0b1
[35:34]	DL2WS	<p>L2 cache Write Streaming no-allocate threshold.</p> <p><b>0b00</b> 16th consecutive streaming cache line does not allocate in the L2 cache.</p> <p><b>0b01</b> 128th consecutive streaming cache line does not allocate in the L2 cache.</p> <p><b>0b10</b> 512th consecutive streaming cache line does not allocate in the L2 cache.</p> <p><b>0b11</b> Disables streaming. All write-allocate lines allocate in the L2 cache.</p>	0b01

Bits	Name	Description	Reset
[33:32]	DL1WS	<p>L1 data cache write streaming no-allocate threshold.</p> <p><b>0b00</b> 4th consecutive streaming cache line does not allocate in the L1 data cache.</p> <p><b>0b01</b> 64th consecutive streaming cache line does not allocate in the L1 data cache.</p> <p><b>0b10</b> 128th consecutive streaming cache line does not allocate in the L1 data cache.</p> <p><b>0b11</b> Disables write streaming detection. All write-allocate lines allocate in the L1 data cache.</p>	0b00
[31:30]	DPEN	<p>L1 data cache prefetcher enable.</p> <p><b>0b00</b> Prefetcher disabled.</p> <p><b>0b01</b> Prefetcher enabled without power-aware throttling. May boost performance in some situations, but consumes more power.</p> <p><b>0b11</b> Prefetcher enabled with power-aware throttling. May limit performance in some situations compared with DPEN == 0b01, but consumes less power.</p> <p>All other values are Reserved.</p>	0b11
[29:27]	DPDEPTH	<p>L1 data cache prefetcher depth.</p> <p><b>0b000</b> Up to 1 outstanding prefetch.</p> <p><b>0b001</b> Up to 2 outstanding prefetches.</p> <p><b>0b010</b> Up to 3 outstanding prefetches.</p> <p><b>0b011</b> Up to 4 outstanding prefetches.</p> <p><b>0b100</b> Up to 5 outstanding prefetches.</p> <p><b>0b101</b> Up to 6 outstanding prefetches.</p> <p><b>0b110</b> Up to 7 outstanding prefetches.</p> <p><b>0b111</b> Up to 8 outstanding prefetches.</p>	0b101

Bits	Name	Description	Reset
[26:25]	DPL2	<p>L1 data cache prefetcher into the L2 behavior.</p> <p><b>0b00</b> Do not prefetch into the L2.</p> <p><b>0b01</b> Initial L2 prefetch is 8 lines ahead of the L1 prefetch.</p> <p><b>0b10</b> Initial L2 prefetch is 16 lines ahead of the L1 prefetch.</p> <p><b>0b11</b> Initial L2 prefetch is 32 lines ahead of the L1 prefetch.</p>	0b10
[24]	TLAC	<p>Tag Lookup Avoidance Cache (TLAC) enable.</p> <p><b>0b0</b> TLAC disabled.</p> <p><b>0b1</b> TLAC enabled.</p>	0b1
[23]	DMB	<p>Data Memory Barrier (DMB) instruction behavior.</p> <p><b>0b0</b> DMB instructions behave as indicated by the Arm architecture.</p> <p><b>0b1</b> DMB instructions behave as DSB instructions (full system barrier).</p> <p>If the value of AArch64-IMP_INTLATENCY_EL2.DMB is not 0 then PE behaves as if the value of the AArch64-IMP_CPUACTLR_EL1.DMB field is 1 for all purposes other than returning the value of a direct read of the field.</p>	0b0
[22:21]	RES0	Reserved	RES0
[20]	WSRST	<p>Write streaming mode reset control. Arm recommends to set this field to 0b1 when accessing memory locations with no Early Write Acknowledgement.</p> <p><b>0b0</b> Write streaming mode will not reset when a specific micro-architectural condition is met.</p> <p><b>0b1</b> Write streaming mode will reset when a specific micro-architectural condition is met.</p>	0b0
[19]	IREPL	<p>L1 instruction cache replacement policy.</p> <p><b>0b0</b> Flexible segregation replacement policy. This replacement policy is designed to reduce pollution caused by excessive speculative fetches from applications with poor locality.</p> <p><b>0b1</b> Pseudo-LRU replacement policy.</p>	0b1



Bits	Name	Description	Reset
[18:17]	IPEN	<p>L1 instruction cache prefetcher enable.</p> <p><b>0b00</b> Prefetcher disabled.</p> <p><b>0b01</b> Prefetcher enabled without power-aware throttling. May boost performance in some situations, but consumes more power.</p> <p><b>0b11</b> Prefetcher enabled with power-aware throttling. May limit performance in some situations compared with IPEN == 0b01, but consumes less power.</p> <p>All other values are Reserved.</p>	0b11
[16:15]	IPDEPTH	<p>L1 instruction cache prefetcher depth.</p> <p><b>0b00</b> Fetch up to 1 line ahead.</p> <p><b>0b01</b> Fetch up to 2 lines ahead.</p> <p><b>0b10</b> Fetch up to 3 lines ahead.</p> <p><b>0b11</b> Fetch up to 4 lines ahead.</p>	0b10
[14]	IPMODE	<p>L1 instruction cache prefetcher mode.</p> <p><b>0b0</b> Early next line mode. The prefetcher aims to always prefetch up to IPDEPTH lines ahead of the current cache line.</p> <p><b>0b1</b> Next line mode. The prefetcher begins prefetching up to IPDEPTH lines ahead only when the current line misses in the cache.</p>	0b0
[13]	IMCWT	<p>L1 instruction cache main cache way tracker control. Cache way tracker is used to minimize power on sequential or known accesses to the cache.</p> <p><b>0b0</b> Main cache way tracker disabled.</p> <p><b>0b1</b> Main cache way tracker enabled.</p>	0b1
[12]	INBTBCWT	<p>L1 instruction cache nano Branch Target Buffer (nBTB) cache way tracker control. Cache way tracker is used to minimize power on sequential or known accesses to the cache.</p> <p><b>0b0</b> nBTB cache way tracker disabled.</p> <p><b>0b1</b> nBTB cache way tracker enabled.</p>	0b1

Bits	Name	Description	Reset
[11]	ICRSCWT	L1 instruction cache CRS cache way tracker control. Cache way tracker is used to minimize power on sequential or known accesses to the cache.  <b>0b0</b> CRS cache way tracker disabled.  <b>0b1</b> CRS cache way tracker enabled.	0b1
[10:9]	IALLOC	L1 instruction cache allocate policy.  <b>0b00</b> Cache allocates instructions fetched from either MM or LLRAM.  <b>0b01</b> Cache allocates instructions fetched from MM, but does not allocate instructions fetched from LLRAM.  <b>0b10</b> Cache allocates instructions fetched from LLRAM, but does not allocate instructions fetched from MM.  <b>0b11</b> Cache does not allocate instructions fetched from either LLRAM or MM.	0b00
[8]	NBTBFLUSH	Nano Branch Target Buffer (nBTB) flushing behavior.  <b>0b0</b> nBTB flushes only as needed.  <b>0b1</b> nBTB flushes as needed, as well as on Context Synchronization, cache maintenance operations, L1I MMS allocations, and parity errors.	0b0
[7]	DGHS	Data Gathering Hint Stalling behavior.  <b>0b0</b> Upon executing a DGH instruction, the store buffer begins draining the existing slots. The pipeline does not stall.  <b>0b1</b> Upon executing a DGH instruction, the store buffer begins draining the existing slots. The pipeline stalls until all pending stores to TCMs have drained. No stalling occurs for pending stores to LLRAM or MM.	0b0
[6]	BUBCL	Bubble Closing behavior. This feature is used to improve IPC by making better use of pipelines in some situations.  <b>0b0</b> The pipeline does not attempt to close bubbles.  <b>0b1</b> The pipeline closes bubbles when possible.	0b1
[5]	FALF	Fast aligned load forwarding control. This feature is used to improve IPC by making forwarding from aligned load faster in some situations.  <b>0b0</b> Fast aligned load forwarding disabled.  <b>0b1</b> Fast aligned load forwarding enabled.	0b1

Bits	Name	Description	Reset
[4]	FPC	Fast pointer chasing control. This feature is used to improve IPC by making load forwarding to base address faster in some situations.  <b>0b0</b> Fast pointer chasing disabled.  <b>0b1</b> Fast pointer chasing enabled.	0b1
[3]	OODIV	Out-of-order division control.  <b>0b0</b> Floating-point divisions complete in-order.  <b>0b1</b> Floating-point divisions complete out-of-order.	0b1
[2:0]	MI	Multi-issuing control.  <b>0b000</b> Instructions can only be issued from slot0.  <b>0b010</b> FP/AdvSIMD instructions can only be issued from slot0. Other instructions can be issued from slot0 or slot1.  <b>0b011</b> All instructions can be issued from slot0 or slot1.  <b>0b110</b> FP/AdvSIMD instructions can only be issued from slot0. Other instructions can be issued from slot0, slot1 or slot2.  <b>0b111</b> All instructions can be issued from slot0, slot1 or slot2.  All other values are Reserved.	0b111

## Access

MRS <Xt>, IMP\_CPUACTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b000

MSR IMP\_CPUACTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b000

## Accessibility

MRS <Xt>, IMP\_CPUACTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    
```

```
else
    X[t, 64] = IMP_CPUACTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUACTLR_EL1;
```

MSR IMP\_CPUACTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.AUX == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUACTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUACTLR_EL1 = X[t, 64];
```

A.2.2.45 IMP\_BPCTLR\_EL1, Branch Predictor Control Register

This register controls in which exception levels the branch predictor is active, and whether the dynamic or static branch predictor is used.

It also controls the behavior of the static branch predictor depending on the branch instructions and their condition code. For those fields, the following abbreviations are used:

- T: taken
- NT: not taken

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

R

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	xx10	xx10	xx10
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-94: AARCH64\_IMP\_BPCTLR\_EL1 bit assignments

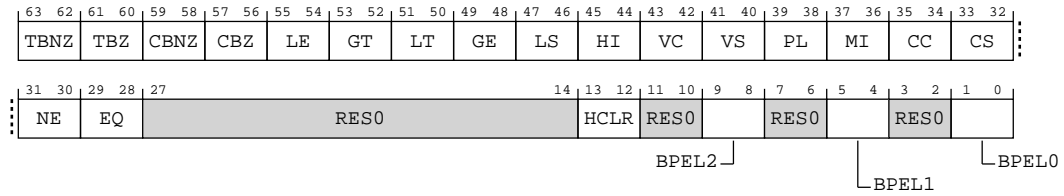


Table A-248: IMP\_BPCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:62]	TBNZ	Static branch predictor behavior for TBNZ instructions.  <b>0b00</b> Predicted NT if offset < 0; predicted NT if offset >= 0. <b>0b01</b> Predicted NT if offset < 0; predicted T if offset >= 0. <b>0b10</b> Predicted T if offset < 0; predicted NT if offset >= 0. <b>0b11</b> Predicted T if offset < 0; predicted T if offset >= 0.	xx
[61:60]	TBZ	Static branch predictor behavior for TBZ instructions.  <b>0b00</b> Predicted NT if offset < 0; predicted NT if offset >= 0. <b>0b01</b> Predicted NT if offset < 0; predicted T if offset >= 0. <b>0b10</b> Predicted T if offset < 0; predicted NT if offset >= 0. <b>0b11</b> Predicted T if offset < 0; predicted T if offset >= 0.	xx
[59:58]	CBNZ	Static branch predictor behavior for CBNZ instructions.  <b>0b00</b> Predicted NT if offset < 0; predicted NT if offset >= 0. <b>0b01</b> Predicted NT if offset < 0; predicted T if offset >= 0. <b>0b10</b> Predicted T if offset < 0; predicted NT if offset >= 0. <b>0b11</b> Predicted T if offset < 0; predicted T if offset >= 0.	xx

Bits	Name	Description	Reset
[57:56]	CBZ	<p>Static branch predictor behavior for CBZ instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[55:54]	LE	<p>Static branch predictor behavior for B.LE instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[53:52]	GT	<p>Static branch predictor behavior for B.GT instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[51:50]	LT	<p>Static branch predictor behavior for B.LT instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx

Bits	Name	Description	Reset
[49:48]	GE	<p>Static branch predictor behavior for B.GE instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[47:46]	LS	<p>Static branch predictor behavior for B.LS instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[45:44]	HI	<p>Static branch predictor behavior for B.HI instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[43:42]	VC	<p>Static branch predictor behavior for B.VC instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx

Bits	Name	Description	Reset
[41:40]	VS	<p>Static branch predictor behavior for B.VS instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[39:38]	PL	<p>Static branch predictor behavior for B.PL instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[37:36]	MI	<p>Static branch predictor behavior for B.MI instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[35:34]	CC	<p>Static branch predictor behavior for B.CC instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx



Bits	Name	Description	Reset
[33:32]	CS	<p>Static branch predictor behavior for B.CS instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[31:30]	NE	<p>Static branch predictor behavior for B.NE instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[29:28]	EQ	<p>Static branch predictor behavior for B.EQ instructions.</p> <p><b>0b00</b> Predicted NT if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b01</b> Predicted NT if offset &lt; 0; predicted T if offset &gt;= 0.</p> <p><b>0b10</b> Predicted T if offset &lt; 0; predicted NT if offset &gt;= 0.</p> <p><b>0b11</b> Predicted T if offset &lt; 0; predicted T if offset &gt;= 0.</p>	xx
[27:14]	RES0	Reserved	RES0
[13:12]	HCLR	<p>Control the flushing to branch history buffers when taking an exception to a higher exception level.</p> <p><b>0b00</b> This control does not cause branch history buffers to be flushed.</p> <p><b>0b01</b> Flush the BTAC on the exception entry.</p> <p><b>0b10</b> Flush the dynamic branch predictor on the exception entry.</p> <p><b>0b11</b> Flush both the dynamic branch predictor and the BTAC on the exception entry.</p>	0b00
[11:10]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[9:8]	BPEL2	<p>Dynamic branch predictor at EL2.</p> <p><b>0b00</b> When running at EL2, no branches are predicted.</p> <p><b>0b01</b> When running at EL2, branches are predicted with the static predictor.</p> <p><b>0b10</b> When running at EL2, branches are predicted with the dynamic predictors.</p> <p><b>0b11</b> When running at EL2, branches are predicted with the dynamic predictors, but the BTAC is disabled. Indirect branches which depend on BTAC are not predicted.</p> <p>Other values are Reserved.</p> <p><b>When PSTATE.EL == EL2</b> Access to this field is: RW</p> <p><b>Otherwise</b> Access to this field is: RO</p>	0b10
[7:6]	RES0	Reserved	RES0
[5:4]	BPEL1	<p>Dynamic branch predictor at EL1.</p> <p><b>0b00</b> When running at EL1, no branches are predicted.</p> <p><b>0b01</b> When running at EL1, branches are predicted with the static predictor.</p> <p><b>0b10</b> When running at EL1, branches are predicted with the dynamic predictors.</p> <p><b>0b11</b> When running at EL1, branches are predicted with the dynamic predictors, but the BTAC is disabled. Indirect branches which depend on BTAC are not predicted.</p> <p>Other values are Reserved.</p>	0b10
[3:2]	RES0	Reserved	RES0
[1:0]	BPELO	<p>Dynamic branch predictor at ELO.</p> <p><b>0b00</b> When running at ELO, no branches are predicted.</p> <p><b>0b01</b> When running at ELO, branches are predicted with the static predictor.</p> <p><b>0b10</b> When running at ELO, branches are predicted with the dynamic predictors.</p> <p><b>0b11</b> When running at ELO, branches are predicted with the dynamic predictors, but the BTAC is disabled. Indirect branches which depend on BTAC are not predicted.</p> <p>Other values are Reserved.</p>	0b10

Access

MRS <Xt>, IMP\_BPCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b11111	0b0001	0b001

MSR IMP\_BPCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b11111	0b0001	0b001

Accessibility

MRS <Xt>, IMP\_BPCTLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_BPCTLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_BPCTLR_EL1;
```

MSR IMP\_BPCTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.BPRED == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_BPCTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_BPCTLR_EL1 = X[t, 64];
```

A.2.2.46 IMP\_CPUBUSTIMEOUTR\_EL1, CPU Bus Timeout Register

This register controls various aspects of bus timeouts.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

**Access type**

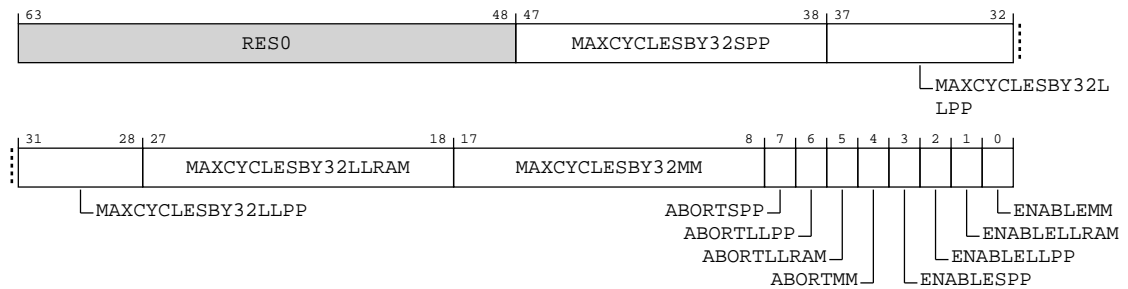
See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-95: AARCH64\_IMP\_CPUBUSTIMEOUTR\_EL1 bit assignments****Table A-251: IMP\_CPUBUSTIMEOUTR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:38]	MAXCYCLESBY32SPP	SPP bus timeout value in SCLK cycles divided by 32.  A write to this field is ignored when AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLESPP == 0b1 and AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLESPP is not being cleared to 0b0 in the same write.  The value 0 is reserved and has no effect.	10{x}
[37:28]	MAXCYCLESBY32LLPP	LLPP bus timeout value in SCLK cycles divided by 32.  A write to this field is ignored when AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLELLPP == 0b1 and AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLELLPP is not being cleared to 0b0 in the same write.  The value 0 is reserved and has no effect.	10{x}

Bits	Name	Description	Reset
[27:18]	MAXCYCLESBY32LLRAM	<p>LLRAM bus timeout value in SCLK cycles divided by 32.</p> <p>A write to this field is ignored when IMP_CPUBUSTIMEOUTR_EL1.ENABLELLRAM == 0b1 and IMP_CPUBUSTIMEOUTR_EL1.ENABLELLRAM is not being cleared to 0b0 in the same write.</p> <p>The value 0 is reserved and has no effect.</p>	10{x}
[17:8]	MAXCYCLESBY32MM	<p>MM bus timeout value in SCLK cycles divided by 32.</p> <p>A write to this field is ignored when AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLEMM == 0b1 and AArch64-IMP_CPUBUSTIMEOUTR_EL1.ENABLEMM is not being cleared to 0b0 in the same write.</p>	10{x}
[7]	ABORTSPP	<p>SPP bus timeout abort behavior.</p> <p><b>0b0</b></p> <p>When SPP bus timeout is detected, continue using the SPP bus.</p> <p><b>0b1</b></p> <p>When SPP bus timeout is detected, abort current and future accesses to the SPP region.</p> <p><b>Note:</b> This control might not have effect when the core is in Debug state.</p>	x
[6]	ABORTLLPP	<p>LLPP bus timeout abort behavior.</p> <p><b>0b0</b></p> <p>When LLPP bus timeout is detected, continue using the LLPP bus.</p> <p><b>0b1</b></p> <p>When LLPP bus timeout is detected, abort current and future accesses to the LLPP region.</p> <p><b>Note:</b> This control might not have effect when the core is in Debug state.</p>	x
[5]	ABORTLLRAM	<p>LLRAM bus timeout abort behavior.</p> <p><b>0b0</b></p> <p>When LLRAM bus timeout is detected, continue using the LLRAM bus.</p> <p><b>0b1</b></p> <p>When LLRAM bus timeout is detected, abort current and future accesses to the LLRAM region.</p> <p><b>Note:</b> This control might not have effect when the core is in Debug state.</p>	x

Bits	Name	Description	Reset
[4]	ABORTMM	MM bus timeout abort behavior.  <b>0b0</b> When MM bus timeout is detected, continue using the MM bus.  <b>0b1</b> When MM bus timeout is detected, abort current and future accesses to the MM region.  <b>Note:</b> This control might not have effect when the core is in Debug state.	x
[3]	ENABLESPP	Timeout counter behavior for the SPP bus.  <b>0b0</b> Timeout counter disabled for the SPP bus.  <b>0b1</b> Timeout counter enabled for the SPP bus.	0b0
[2]	ENABLELLPP	Timeout counter behavior for the LLPP bus.  <b>0b0</b> Timeout counter disabled for the LLPP bus.  <b>0b1</b> Timeout counter enabled for the LLPP bus.	0b0
[1]	ENABLELLRAM	Timeout counter behavior for the LLRAM bus.  <b>0b0</b> Timeout counter disabled for the LLRAM bus.  <b>0b1</b> Timeout counter enabled for the LLRAM bus.	0b0
[0]	ENABLEMM	Timeout counter behavior for the MM bus.  <b>0b0</b> Timeout counter disabled for the MM bus.  <b>0b1</b> Timeout counter enabled for the MM bus.	0b0

### Access

MRS &lt;Xt&gt;, IMP\_CPUBUSTIMEOUTR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b010

MSR IMP\_CPUBUSTIMEOUTR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b010

## Accessibility

MRS <Xt>, IMP\_CPUBUSTIMEOUTR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUBUSTIMEOUTR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CPUBUSTIMEOUTR_EL1;

```

MSR IMP\_CPUBUSTIMEOUTR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.DIAGNOSTIC == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUBUSTIMEOUTR_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_CPUBUSTIMEOUTR_EL1 = X[t, 64];

```

### A.2.2.47 IMP\_INTMONR\_EL1, Interrupt Monitoring Register

This register supports two modes of operation: maximum value monitor mode and watchdog mode.

- In maximum value monitor mode: a counter keeps track of how much time the processor spends with masked interrupts and/or in WFI/WFE state. The INTMSKCYCLESBY32 and/or WFXCYCLESBY512 fields are updated with the maximum value the counter reached. Software can read these fields to monitor the processor behavior.
- In watchdog mode: software programs the INTMSKCYCLESBY32 and/or WFXCYCLESBY512 fields. These fields act as upper limits. If the processor spends more time with masked interrupts and/or in WFI/WFE state than the programmed limits, the error is reported through RAS. Errors are reported for masked interrupts only if any of the IRQ, FIQ, or SEI control bits are set. Errors are reported for WFI/WFE state only if any of the WFI or WFE control bits are set.

In both modes of operation, the IRQ, FIQ and SEI fields control whether the counter tracks the time which the processor spends with masked interrupts. The WFI and WFE fields control whether the counter tracks the time which the processor spends in WFI/WFE state. The counter which counts in SCLK cycles is able to keep counting, regardless of whether the CPU clock has been switched off in WFI/WFE low-power state. Specifically, the counter works as follows:

- When none of the IRQ, FIQ, SEI, WFI and WFE are set:
  - The counter is in the stopped state
- When any of the IRQ, FIQ or SEI are set, and none of the WFI and WFE are set:
  - If the counter is in the stopped state, when any of the programmed interrupts become masked (but not because of ext-EDSCR.INTdis), the counter resets to 0 and begins counting

- When all of the programmed interrupts become unmasked, the counter stops counting
- When any of the WFI or WFE are set, and none of the IRQ, FIQ and SEI are set:
  - When the core enters the programmed WFx state, the counter resets to 0 and begins counting
  - When the core exits the programmed WFx state, the counter stops counting
- When any of the IRQ, FIQ or SEI and any of the WFI or WFE are set:
  - If the counter is in the stopped state, when any of the programmed interrupts become masked (but not because of ext-EDSCR.INTdis), the counter resets to 0 and begins counting
  - When all of the programmed interrupts are already unmasked and the core enters the programmed WFx state, the counter resets to 0 and begins counting
  - When all of the programmed interrupts are already unmasked and the core exits the programmed WFx state, the counter stops counting
  - When all of the programmed interrupts become unmasked, the counter stops counting
- When there is a write to IMP\_INTMONR\_EL1, the counter resets to 0.

The counter behavior described above allows the programmer to use IMP\_INTMONR\_EL1 for three purposes:

- To monitor for how long the core is unable to take interrupts. The type of interrupts is programmed using the IRQ, FIQ and SEI fields. The related time period is in the INTMSKCYCLESBY32 field.
- To monitor for how long the core is in WFx state. The type of WFx state is programmed using the WFI and WFE fields. The related time period is in the WFXCYCLESBY512 field.
- To monitor for how long the core is unable to take interrupts, and for how long the core is in WFx state. Being unable to take interrupts is a more significant condition, and it is prioritized compared to WFx state. Therefore, being in WFx state is only counted provided the core is already able to take interrupts. The type of interrupts is programmed using the IRQ, FIQ and SEI fields and the type of WFx state is programmed using the WFI and WFE fields. The time period of being unable to take interrupts is in the INTMSKCYCLESBY32 field, and the time period of being in WFx state (while able of taking interrupts) is in the WFXCYCLESBY512 field.

In maximum value monitor mode, when the counter reaches its wrap-around threshold (8,160 cycles when using the INTMSKCYCLESBY32 field, or 130,560 cycles when using the WFXCYCLESBY512 field), the related field saturates and retains this value as the maximum value.



The counting for masked interrupts is accurate to +1/-1 from the value specified in the INTMSKCYCLESBY32 field.

---

## Configurations

This register is available in all configurations.



Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	0000	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-96: AARCH64\_IMP\_INTMONR\_EL1 bit assignments

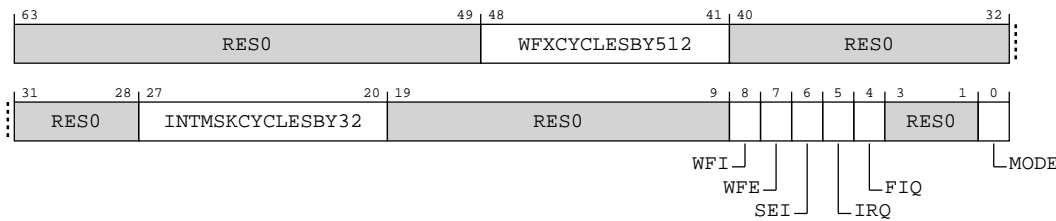


Table A-254: IMP\_INTMONR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:49]	RES0	Reserved	RES0
[48:41]	WFXCYCLESBY512	WFI/WFE maximum cycle count divided by 512.  When the maximum value monitor mode is selected, the write to this field is ignored, and the read returns the counter value if the WFI/WFE monitoring is enabled or zero otherwise.	8 {x}
[40:28]	RES0	Reserved	RES0
[27:20]	INTMSKCYCLESBY32	Masked interrupts maximum cycle count divided by 32.  When the maximum value monitor mode is selected, the write to this field is ignored, and the read returns the counter value if the masked interrupts monitoring is enabled or zero otherwise.	8 {x}
[19:9]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[8]	WFI	<p>Count time when in WFI state.</p> <p><b>0b0</b></p> <p>Do not increment the counter when the core is in WFI state. Do not report WFI errors in watchdog mode.</p> <p><b>0b1</b></p> <p>Increment the counter when the core is in WFI state. Report WFI errors in watchdog mode.</p>	0b0
[7]	WFE	<p>Count time when in WFE state.</p> <p><b>0b0</b></p> <p>Do not increment the counter when the core is in WFE state. Do not report WFE errors in watchdog mode.</p> <p><b>0b1</b></p> <p>Increment the counter when the core is in WFE state. Report WFE errors in watchdog mode.</p>	0b0
[6]	SEI	<p>SError interrupt behavior.</p> <p><b>0b0</b></p> <p>Do not increment the counter when SError interrupts are masked. Do not report SError errors in watchdog mode.</p> <p><b>0b1</b></p> <p>Increment the counter when SError interrupts are masked. Report SError errors in watchdog mode.</p> <p>This field is ignored when the core is in Debug state.</p>	0b0
[5]	IRQ	<p>IRQ interrupt behavior.</p> <p><b>0b0</b></p> <p>Do not increment the counter when IRQ interrupts are masked. Do not report IRQ errors in watchdog mode.</p> <p><b>0b1</b></p> <p>Increment the counter when IRQ interrupts are masked. Report IRQ errors in watchdog mode.</p> <p>This field is ignored when the core is in Debug state.</p>	0b0
[4]	FIQ	<p>FIQ interrupt behavior.</p> <p><b>0b0</b></p> <p>Do not increment the counter when FIQ interrupts are masked. Do not report FIQ errors in watchdog mode.</p> <p><b>0b1</b></p> <p>Increment the counter when FIQ interrupts are masked. Report FIQ errors in watchdog mode.</p> <p>This field is ignored when the core is in Debug state.</p>	0b0
[3:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	MODE	Counter mode.  <b>0b0</b> Watchdog mode.  <b>0b1</b> Maximum value monitor mode.	0b0

### Access

MRS <Xt>, IMP\_INTMONR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b011

MSR IMP\_INTMONR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b011

### Accessibility

MRS <Xt>, IMP\_INTMONR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_INTMONR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_INTMONR_EL1;

```

MSR IMP\_INTMONR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.DIAGNOSTIC == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_INTMONR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_INTMONR_EL1 = X[t, 64];

```

## A.2.2.48 IMP\_MEMPROTCTLR\_EL1, Memory Protection Control Register

This register controls the memory protection, bus protection and transient fault protection features of the CPU.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-97: AARCH64\_IMP\_MEMPROTCTLR\_EL1 bit assignments

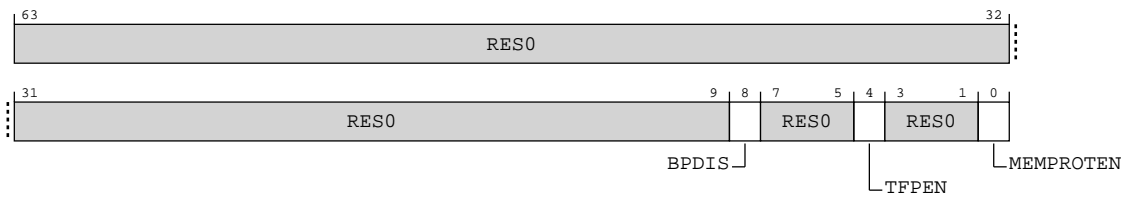


Table A-257: IMP\_MEMPROTCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:9]	RES0	Reserved	RES0
[8]	BPDIS	Bus protection error logging disable.  0b0      Bus protection error logging enabled.  0b1      Bus protection error logging disabled.	0b0
[7:5]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[4]	TFPEN	<p><b>When FLOP_PARITY == 1</b></p> <p>Transient Fault Protection (TFP) error reporting and logging enable.</p> <p>When disabled, the core behaves as if TFP error detection is disabled, and no TFP errors are reported to RAS or signaled to CORETFPFAULT output pin.</p> <p><b>0b0</b></p> <p>TFP error reporting disabled.</p> <p><b>0b1</b></p> <p>TFP error reporting enabled.</p> <p><b>Otherwise</b></p> <p>RES0</p>	<p><b>When the CFGTFPEN configuration pin is HIGH</b></p> <p>'1'</p> <p><b>When the CFGTFPEN configuration pin is LOW</b></p> <p>'0'</p>
[3:1]	RES0	Reserved	RES0
[0]	MEMPROTEN	<p>Memory protection enable.</p> <p><b>0b0</b></p> <p>Structures required to support internal RAM protection functionality are turned off.</p> <p><b>0b1</b></p> <p>Structures required to support internal RAM protection functionality are turned on.</p> <ul style="list-style-type: none"> <li>This field must not be programmed while the caches are enabled, otherwise the behavior of the processor memory system becomes <b>UNPREDICTABLE</b>. Software must ensure that the processor caches are disabled before programming this field. After programming this field, software must ensure that the caches are invalidated before they can be enabled again.</li> <li>If the values of AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN for all cores in the processor cluster are not the same, it is possible for wrong data values to be consumed by any core in the cluster, because errors that are locally suppressed by disabling RAM protection may spread through hardware data coherency mechanisms. Arm recommends that AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and all AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN fields are programmed with the same value, unless otherwise directed by Arm.</li> </ul>	x

## Access

MRS <Xt>, IMP\_MEMPROTCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b101

MSR IMP\_MEMPROTCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0001	0b101

## Accessibility

MRS <Xt>, IMP\_MEMPROTCTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_MEMPROTCTLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_MEMPROTCTLR_EL1;

```

MSR IMP\_MEMPROTCTLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.DIAGNOSTIC == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_MEMPROTCTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_MEMPROTCTLR_EL1 = X[t, 64];

```

### A.2.2.49 IMP\_CPUCFR\_EL1, CPU Configuration Register

This register shows the value of the (not otherwise software-visible) rendering-time parameters and integration-time pin tie-offs, used to configure this CPU core.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic System Control

##### Access type

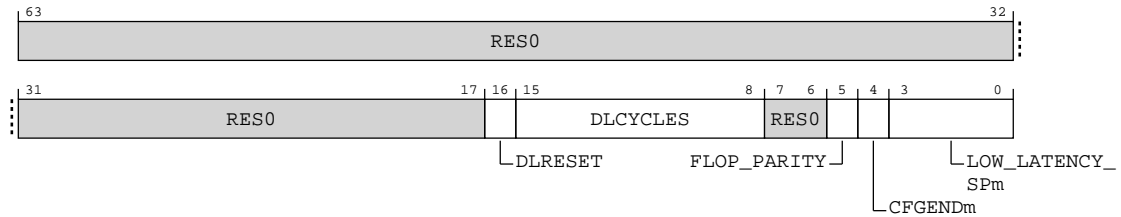
See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-98: AARCH64\_IMP\_CPUCFR\_EL1 bit assignments****Table A-260: IMP\_CPUCFR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:17]	RES0	Reserved	RES0
[16]	DLRESET	Activation of SBIST out of reset deadlock checking. This field takes the value of the DLRESET configuration pin.  <b>0b0</b> The processor does not activate SBIST out of reset deadlock checking.  <b>0b1</b> The processor activates SBIST out of reset deadlock checking.	x
[15:8]	DLCYCLES	The value loaded into the FCTLR.FREQ field for the SBIST out of reset deadlock checking. This field takes the value of the DLCYCLES configuration pin.	8 { x }
[7:6]	RES0	Reserved	RES0
[5]	FLOP_PARITY	Flop parity for transient fault protection. This field takes the value of the FLOP_PARITY parameter.  <b>0b0</b> The processor does not implement flop parity.  <b>0b1</b> The processor implements flop parity.	x
[4]	CFGENDm	Endianess out of reset. This field takes the value of the CFGENDm configuration pin.  <b>0b0</b> Explicit data accesses and translation table walks set to little-endian out of reset (SCTLR_EL2.EE and SCTLR_EL1.EE fields).  <b>0b1</b> Explicit data accesses and translation table walks set to big-endian out of reset (SCTLR_EL2.EE and SCTLR_EL1.EE fields).	x

Bits	Name	Description	Reset
[3:0]	LOW_LATENCY_SPm	Low-latency Single-Precision Floating-Point. This field takes the value of the per-core LOW_LATENCY_SPm parameter.  <b>0b0000</b> The core does not implement any special hardware for SP FP operations.  <b>0b0001</b> The core implements additional hardware that supports 3-cycle non-vector SP FP operations.	xxxx

Access

MRS <Xt>, IMP\_CPUCFR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b000

Accessibility

MRS <Xt>, IMP\_CPUCFR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUCFR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CPUCFR_EL1;
```

A.2.2.50 IMP\_CPUPWRCTLR\_EL1, CPU Power Control Register

This register controls various power aspects of the core.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

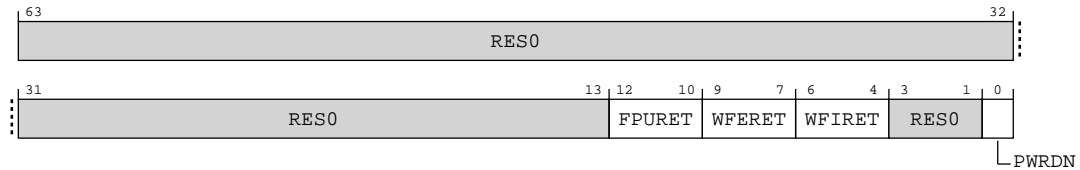
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	0000	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-99: AARCH64\_IMP\_CPUPWRCTLR\_EL1 bit assignments****Table A-262: IMP\_CPUPWRCTLR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:13]	RES0	Reserved	RES0
[12:10]	FPURET	<p><b>When NEON_FPM &gt; 0</b></p> <p>FPU retention control.</p> <p><b>0b000</b> FPU retention disabled.</p> <p><b>0b001</b> When the FPU is idle, request transition to FUNC_RET after 2 timer ticks (40 ns - 200 ns).</p> <p><b>0b010</b> When the FPU is idle, request transition to FUNC_RET after 8 timer ticks (160 ns - 800 ns).</p> <p><b>0b011</b> When the FPU is idle, request transition to FUNC_RET after 32 timer ticks (640 ns - 3.2 us).</p> <p><b>0b100</b> When the FPU is idle, request transition to FUNC_RET after 64 timer ticks (1.28 us - 6.4 us).</p> <p><b>0b101</b> When the FPU is idle, request transition to FUNC_RET after 128 timer ticks (2.56 us - 12.8 us).</p> <p><b>0b110</b> When the FPU is idle, request transition to FUNC_RET after 256 timer ticks (5.12 us - 25.6 us).</p> <p><b>0b111</b> When the FPU is idle, request transition to FUNC_RET after 512 timer ticks (10.24 us - 51.2 us).</p> <p>The time range estimations are given assuming an architectural timer clock frequency between 50 MHz - 10 MHz.</p> <p><b>Otherwise</b> RES0</p>	'000'

Bits	Name	Description	Reset
[9:7]	WFERET	<p>Wait for Event retention control.</p> <p><b>0b000</b> Core retention disabled for WFE.</p> <p><b>0b001</b> When the core enters WFE state, request transition to FULL_RET after 2 timer ticks (40 ns - 200 ns).</p> <p><b>0b010</b> When the core enters WFE state, request transition to FULL_RET after 8 timer ticks (160 ns - 800 ns).</p> <p><b>0b011</b> When the core enters WFE state, request transition to FULL_RET after 32 timer ticks (640 ns - 3.2 us).</p> <p><b>0b100</b> When the core enters WFE state, request transition to FULL_RET after 64 timer ticks (1.28 us - 6.4 us).</p> <p><b>0b101</b> When the core enters WFE state, request transition to FULL_RET after 128 timer ticks (2.56 us - 12.8 us).</p> <p><b>0b110</b> When the core enters WFE state, request transition to FULL_RET after 256 timer ticks (5.12 us - 25.6 us).</p> <p><b>0b111</b> When the core enters WFE state, request transition to FULL_RET after 512 timer ticks (10.24 us - 51.2 us).</p> <p>The time range estimations are given assuming an architectural timer clock frequency between 50 MHz - 10 MHz.</p>	0b000

Bits	Name	Description	Reset
[6:4]	WFIRET	<p>Wait for Interrupt retention control.</p> <p><b>0b000</b> Core retention disabled for WFI.</p> <p><b>0b001</b> When the core enters WFI state, request transition to FULL_RET after 2 timer ticks (40 ns - 200 ns).</p> <p><b>0b010</b> When the core enters WFI state, request transition to FULL_RET after 8 timer ticks (160 ns - 800 ns).</p> <p><b>0b011</b> When the core enters WFI state, request transition to FULL_RET after 32 timer ticks (640 ns - 3.2 us).</p> <p><b>0b100</b> When the core enters WFI state, request transition to FULL_RET after 64 timer ticks (1.28 us - 6.4 us).</p> <p><b>0b101</b> When the core enters WFI state, request transition to FULL_RET after 128 timer ticks (2.56 us - 12.8 us).</p> <p><b>0b110</b> When the core enters WFI state, request transition to FULL_RET after 256 timer ticks (5.12 us - 25.6 us).</p> <p><b>0b111</b> When the core enters WFI state, request transition to FULL_RET after 512 timer ticks (10.24 us - 51.2 us).</p> <p>The time range estimations are given assuming an architectural timer clock frequency between 50 MHz - 10 MHz.</p>	0b000
[3:1]	RES0	Reserved	RES0
[0]	PWRDN	<p>Indicates to the power controller if the core wants to power down when it enters WFI state.</p> <p><b>0b0</b> When the core enters WFI state, do not request to power down.</p> <p><b>0b1</b> When the core enters WFI state, request to power down.</p>	0b0

## Access

MRS <Xt>, IMP\_CPUPWRCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b111

MSR IMP\_CPUPWRCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b111

## Accessibility

MRS <Xt>, IMP\_CPUPWRCTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPWRCTLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPWRCTLR_EL1;

```

MSR IMP\_CPUPWRCTLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.POWER == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPWRCTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_CPUPWRCTLR_EL1 = X[t, 64];

```

### A.2.2.51 IMP\_CLUSTERCFR\_EL1, Cluster Configuration Register

This register shows the value of the (not otherwise software-visible) rendering-time parameters and integration-time pin tie-offs, used to configure the processor cluster.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Generic System Control

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

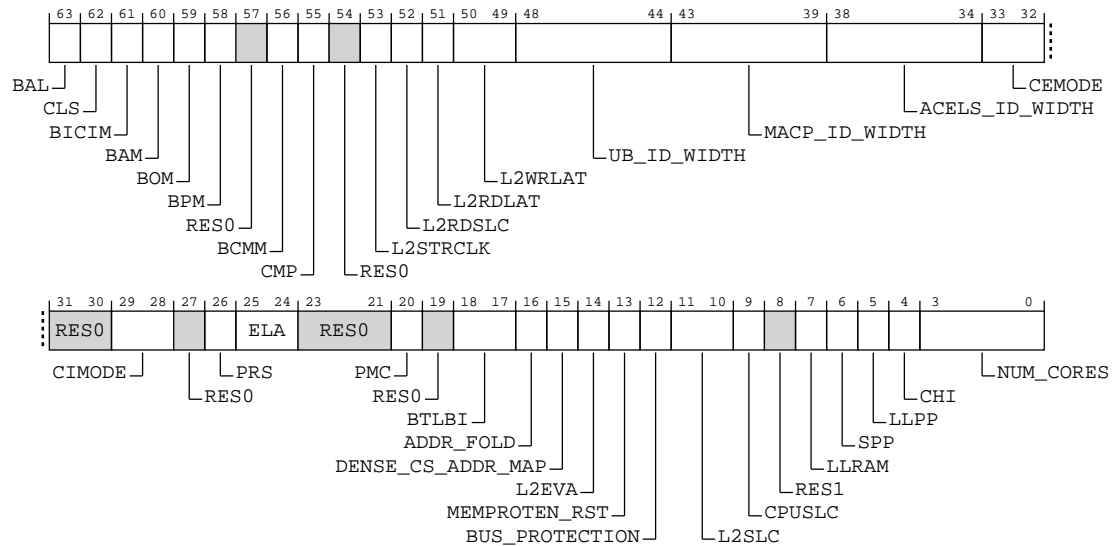


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-100: AARCH64\_IMP\_CLUSTERCFR\_EL1 bit assignments**



**Table A-265: IMP\_CLUSTERCFR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63]	BAL	Broadcast Atomic LLRAM. This field takes the value of the BROADCASTATOMICL configuration pin.  <b>0b0</b> Atomic transactions on the LLRAM port are not sent externally.  <b>0b1</b> Atomic transactions on the LLRAM port are sent externally.	x
[62]	CLS	Configuration LLRAM Shared. This field takes the value of the CFGLLRAMSHARED configuration pin.  <b>0b0</b> Shareable transactions on the LLRAM port are not broadcast externally.  <b>0b1</b> Shareable transactions on the LLRAM port are broadcast externally.	x

Bits	Name	Description	Reset
[61]	BICIM	<p><b>When CHI == 1</b> Broadcast Instruction Cache Invalidate Main Manager. This field takes the value of the BROADCASTICINVALM configuration pin.</p> <p><b>0b0</b> Instruction cache DVM transactions on the Main Manager port are not sent externally.</p> <p><b>0b1</b> Instruction cache DVM transactions on the Main Manager port are sent externally.</p> <p><b>Otherwise</b> RES0</p>	x
[60]	BAM	<p>Broadcast Atomic Main Manager. This field takes the value of the BROADCASTATOMICM configuration pin.</p> <p><b>0b0</b> Atomic transactions on the Main Manager port are not sent externally.</p> <p><b>0b1</b> Atomic transactions on the Main Manager port are sent externally.</p>	x
[59]	BOM	<p><b>When CHI == 1</b> Broadcast Outer Main Manager. This field takes the value of the BROADCASTOUTERM configuration pin.</p> <p><b>0b0</b> Shareable transactions on the Main Manager port are not broadcast externally.</p> <p><b>0b1</b> Shareable transactions on the Main Manager port are broadcast externally.</p> <p><b>Otherwise</b> RES0</p>	x
[58]	BPM	<p><b>When CHI == 1</b> Broadcast Persist Maintenance Main Manager. This field takes the value of the BROADCASTPERSISTM configuration pin.</p> <p><b>0b0</b> On the Main Manager port, DC CVAP instructions are treated the same as DC CVAC.</p> <p><b>0b1</b> On the Main Manager port, DC CVAP instructions are sent as a clean to the point of persistence transactions.</p> <p><b>Otherwise</b> RES0</p>	x
[57]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[56]	BCMM	<p><b>When CHI == 1</b></p> <p>Broadcast Cache Maintenance Main Manager. This field takes the value of the BROADCASTCACHEMAINTM configuration pin.</p> <p><b>0b0</b></p> <p>Cache maintenance operations are not broadcast to downstream caches on the Main Manager port.</p> <p><b>0b1</b></p> <p>Cache maintenance operations are broadcast to downstream caches on the Main Manager port.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[55]	CMP	<p>Main Manager port poison support. This field takes the value of the CFGMMPOISON configuration pin.</p> <p><b>0b0</b></p> <p>Main Manager port does not support poison.</p> <p><b>0b1</b></p> <p>Main Manager port supports poison.</p>	x
[54]	RES0	Reserved	RES0
[53]	L2STRCLK	<p>L2 cache Stretch Clock. This field takes the value of the L2_DATA_STRETCH_CLK global parameter.</p> <p><b>0b0</b></p> <p>L2 data RAMs clock not stretched. The clock pulse will be high for half an SCLK cycle.</p> <p><b>0b1</b></p> <p>L2 data RAMs clock stretched. The clock pulse will be high for a whole SCLK cycle.</p>	x
[52]	L2RDSLC	<p>L2 cache Read Slice. This field takes the value of the L2_DATA_RD_SLICE global parameter.</p> <p><b>0b0</b></p> <p>No register slice present for reading the L2 data RAMs.</p> <p><b>0b1</b></p> <p>Register slice present for reading the L2 data RAMs.</p>	x
[51]	L2RDLAT	<p>L2 cache Read Latency. This field takes the value of the L2_DATA_RD_LATENCY global parameter.</p> <p><b>0b0</b></p> <p>2 cycles output delay from L2 data RAMs.</p> <p><b>0b1</b></p> <p>3 cycles output delay from L2 data RAMs.</p>	x
[50:49]	L2WRLAT	<p>L2 cache Write Latency. This field takes the value of the L2_DATA_WR_LATENCY global parameter.</p> <p><b>0b00</b></p> <p>1 cycle input delay from L2 data RAMs.</p> <p><b>0b01</b></p> <p>2 cycles input delay from L2 data RAMs.</p> <p><b>0b10</b></p> <p>2 cycles input delay plus 1 cycle hold from L2 data RAMs.</p>	xx

Bits	Name	Description	Reset
[48:44]	UB_ID_WIDTH	Utility Bus port AXI ID Width. This field takes the value of the UB_ID_WIDTH global parameter.	5 {x}
[43:39]	MACP_ID_WIDTH	MACP AXI ID Width. This field takes the value of the MACP_ID_WIDTH global parameter.	5 {x}
[38:34]	ACELS_ID_WIDTH	ACELS port AXI ID Width. This field takes the value of the ACELS_ID_WIDTH global parameter.	5 {x}
[33:32]	CEMODE	<p>Cluster Execution Mode select. This field takes the value of the CFGCEMODE configuration pins. It determines which comparisons are active at boot time.</p> <p><b>0b01</b> Split-mode. All physical cores run independently of each other. Cluster shadow logic is non-existent or inactive. Value allowed with any CIMODE.</p> <p><b>0b10</b> Hybrid-mode. All physical cores run independently of each other. Cluster units are compared against their shadow ones. Value allowed when CIMODE is 0b01 or 0b11.</p> <p><b>0b11</b> Lock-mode. Physical cores are compared within pairs. Cluster units are compared against their shadow ones. Value allowed when CIMODE is 0b10 or 0b11.</p> <p>For safety reasons, illegal CFGCEMODE values will be ignored by the processor. All implemented comparators will be activated instead.</p>	xx
[31:30]	RES0	Reserved	RES0
[29:28]	CIMODE	<p>Cluster Implementation Mode. This field takes the value of the CIMODE global parameter. It determines which comparison capabilities are implemented by the processor.</p> <p><b>0b00</b> Split-mode only. No comparison logic implemented. The processor can only operate in Split-mode. CEMODE must be 0b01.</p> <p><b>0b01</b> Split-mode/Hybrid-mode. Comparison logic implemented for the cluster. The processor can operate in Split-mode or Hybrid-mode. CEMODE must be 0b01 or 0b10.</p> <p><b>0b10</b> Split-mode/Lock-mode. Comparison logic implemented for the cores and the cluster. The processor can operate in Split-mode or Lock-mode. CEMODE must be 0b01 or 0b11.</p> <p><b>0b11</b> Split-mode/Hybrid-mode/Lock-mode. Comparison logic implemented for the cores and the cluster. The processor can operate in Split-mode, Hybrid-mode or Lock-mode. CEMODE must be 0b01, 0b10 or 0b11.</p>	xx
[27]	RES0	Reserved	RES0
[26]	PRS	<p>PPU Reset State. This field takes the value of the PPU_RST_STATE global parameter.</p> <p><b>0b0</b> Power Policy Units stay in OFF state after reset.</p> <p><b>0b1</b> Power Policy Units transition to ON after reset.</p>	x



Bits	Name	Description	Reset
[25:24]	ELA	<p>Embedded Logic Analyzer. This field depends on the value of the ELA global parameter and the ELADISABLE configuration pin.</p> <p><b>0b00</b></p> <p>The processor does not implement any embedded logic analyzers.</p> <p><b>0b01</b></p> <p>The processor is implemented with embedded CoreSight ELA-600 embedded logic analyzers. The analyzers are disabled and cannot be used.</p> <p><b>0b11</b></p> <p>The processor is implemented with embedded CoreSight ELA-600 embedded logic analyzers. The analyzers are available to be used.</p>	xx
[23:21]	RES0	Reserved	RES0
[20]	PMC	<p>Programmable MBIST Controllers. This field takes the value of the PMC global parameter.</p> <p><b>0b0</b></p> <p>The processor does not implement any programmable MBIST controllers.</p> <p><b>0b1</b></p> <p>The processor is implemented with programmable MBIST controllers to support online MBIST functionality.</p>	x
[19]	RES0	Reserved	RES0
[18:17]	BTLBI	<p><b>When CHI == 1</b></p> <p>Broadcast TLBI Main Manager. BTLBI[0] takes the value of the BROADCASTTLBIINNERM configuration pin and BTLBI[1] takes the value of the BROADCASTTLBIOUTERM configuration pin.</p> <p><b>0b00</b></p> <p>No TLBI operations are broadcast outside the cluster.</p> <p><b>0b01</b></p> <p>Illegal configuration.</p> <p><b>0b10</b></p> <p>Out Shareable TLBI operations are broadcast outside the cluster.</p> <p><b>0b11</b></p> <p>Both Inner Shareable TLBI operations and Out Shareable TLBI operations are broadcast outside the cluster.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xx
[16]	ADDR_FOLD	<p>Address folding. This field takes the value of the ADDR_FOLD global parameter.</p> <p><b>0b0</b></p> <p>Processor does not implement the address folding.</p> <p><b>0b1</b></p> <p>Processor implements the address folding.</p>	x

Bits	Name	Description	Reset
[15]	DENSE_CS_ADDR_MAP	Dense memory map for Utility Bus and Debug port. This field takes the value of the DENSE_CS_ADDR_MAP global parameter.  <b>0b0</b> Processor implements the sparse memory map.  <b>0b1</b> Processor implements the dense memory map.	x
[14]	L2EVA	L2 cache POP RAM allocate evict behavior. This field takes the value of the CFGL2EVAIMP configuration pin.  <b>0b0</b> If using POP RAMs, processor does not implement the optimized read/write allocate evict mechanism.  <b>0b1</b> If using POP RAMs, processor is implemented with the optimized read/write allocate evict mechanism.	x
[13]	MEMPROTEN_RST	Reset values of AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN. This field takes the value of the CFGGRAMPROTEN configuration pin.  <b>0b0</b> Reset values of AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN are 0b0.  <b>0b1</b> Reset values of AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN are 0b1.	x
[12]	BUS_PROTECTION	Bus protection. This field takes the value of the BUS_PROTECTION global parameter.  <b>0b0</b> The processor does not implement any structures to protect buses.  <b>0b1</b> The processor is implemented with structures required to support bus protection functionality.	x
[11:10]	L2SLC	L2 Slices and RAM partitions. This field takes the value of the L2_SLICES global parameter.  <b>0b01</b> The L2 cache implements a single slice and a single RAM partition.  <b>0b10</b> The L2 cache implements two slices and two RAM partitions.	xx
[9]	CPUSLC	Extra register slices between the cores and the cluster logic. This field takes the value of the CPU_SLICE global parameter.  <b>0b0</b> No additional register slices exist between the cores and cluster logic.  <b>0b1</b> One additional register slice exists between the cores and cluster logic.	x
[8]	RES1	Reserved	RES1

Bits	Name	Description	Reset
[7]	LLRAM	LLRAM interface. This field takes the value of the LLRAM global parameter.  <b>0b0</b> LLRAM interface is not implemented, and associated hardware logic is not present.  <b>0b1</b> LLRAM interface is implemented.	x
[6]	SPP	SPP interface. This field takes the value of the SPP global parameter.  <b>0b0</b> SPP interface is not implemented, and associated hardware logic is not present.  <b>0b1</b> SPP interface is implemented.	x
[5]	LLPP	LLPP interface. This field takes the value of the LLPP global parameter.  <b>0b0</b> LLPP interface is not implemented, and associated hardware logic is not present.  <b>0b1</b> LLPP interface is implemented.	x
[4]	CHI	Main Manager port type. This field takes the value of the CHI global parameter.  <b>0b0</b> The MM port implements an AXI5 interface.  <b>0b1</b> The MM port implements a CHI.E interface.	x
[3:0]	NUM_CORES	Number of logical CPU cores in the cluster. This field takes the value of the NUM_CORES global parameter divided by 2 when CEMODE == 0b11 or the value of the NUM_CORES global parameter otherwise.  <b>0b0001</b> 1 CPU core implemented in the cluster.  <b>0b0010</b> 2 CPU cores implemented in the cluster.  <b>0b0011</b> 3 CPU cores implemented in the cluster.  <b>0b0100</b> 4 CPU cores implemented in the cluster.  <b>0b0101</b> 5 CPU cores implemented in the cluster.  <b>0b0110</b> 6 CPU cores implemented in the cluster.  <b>0b0111</b> 7 CPU cores implemented in the cluster.  <b>0b1000</b> 8 CPU cores implemented in the cluster.	xxxx

## Access

MRS <Xt>, IMP\_CLUSTERCFR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b000

Accessibility

MRS <Xt>, IMP\_CLUSTERCFR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERCFR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERCFR_EL1;
```

A.2.2.52 IMP\_CLUSTERBUSTIMEOUTR\_EL1, Cluster Bus Timeout Register

This register controls various aspects of bus timeouts.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-101: AARCH64\_IMP\_CLUSTERBUSTIMEOUTR\_EL1 bit assignments

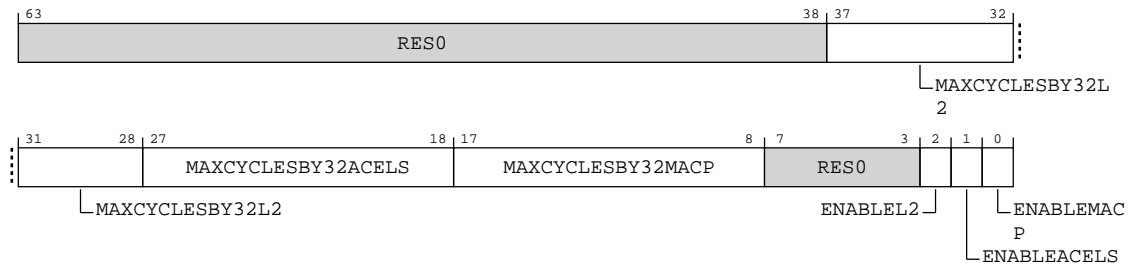


Table A-267: IMP\_CLUSTERBUSTIMEOUTR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:38]	RES0	Reserved	RES0
[37:28]	MAXCYCLESBY32L2	<p>L2 bus timeout value in SCLK cycles divided by 32.</p> <p>A write to this field is ignored when IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEL2 == 0b1 and IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEL2 is not being cleared to 0b0 in the same write.</p> <p>The value 0 is reserved and has no effect.</p>	10{x}
[27:18]	MAXCYCLESBY32ACELS	<p>ACELS bus timeout value in SCLK cycles divided by 32.</p> <p>A write to this field is ignored when IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEACELS == 0b1 and IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEACELS is not being cleared to 0b0 in the same write.</p> <p>The value 0 is reserved and has no effect.</p>	10{x}
[17:8]	MAXCYCLESBY32MACP	<p>MACP bus timeout value in SCLK cycles divided by 32.</p> <p>A write to this field is ignored when IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEMACP == 0b1 and IMP_CLUSTERBUSTIMEOUTR_EL1.ENABLEMACP is not being cleared to 0b0 in the same write.</p> <p>The value 0 is reserved and has no effect.</p>	10{x}
[7:3]	RES0	Reserved	RES0
[2]	ENABLEL2	<p>Timeout counter behavior for the L2 bus.</p> <p><b>0b0</b></p> <p>Timeout counter disabled for the L2 bus.</p> <p><b>0b1</b></p> <p>Timeout counter enabled for the L2 bus.</p>	0b0
[1]	ENABLEACELS	<p>Timeout counter behavior for the ACELS bus.</p> <p><b>0b0</b></p> <p>Timeout counter disabled for the ACELS bus.</p> <p><b>0b1</b></p> <p>Timeout counter enabled for the ACELS bus.</p>	0b0

Bits	Name	Description	Reset
[0]	ENABLEMACP	Timeout counter behavior for the MACP bus.  <b>0b0</b> Timeout counter disabled for the MACP bus.  <b>0b1</b> Timeout counter enabled for the MACP bus.	0b0

### Access

MRS &lt;Xt&gt;, IMP\_CLUSTERBUSTIMEOUTR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b010

MSR IMP\_CLUSTERBUSTIMEOUTR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b010

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERBUSTIMEOUTR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERBUSTIMEOUTR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERBUSTIMEOUTR_EL1;

```

MSR IMP\_CLUSTERBUSTIMEOUTR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.DIAGNOSTIC == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERBUSTIMEOUTR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERBUSTIMEOUTR_EL1 = X[t, 64];

```

## A.2.2.53 IMP\_CLUSTERACTLR\_EL1, Cluster Auxiliary Control Register

This register contains control bits that affect the cluster behavior.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xx11	xxx1	xx0x	xx00	0001	xxxx	xx00	001x
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-102: AARCH64\_IMP\_CLUSTERACTLR\_EL1 bit assignments

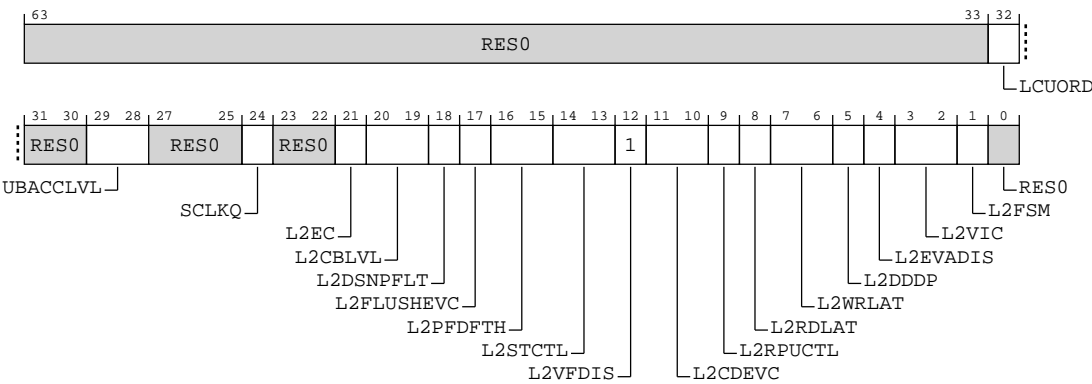


Table A-270: IMP\_CLUSTERACTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:33]	RES0	Reserved	RES0
[32]	LCUORD	LCU Ordering behavior.  0b0 Normal behavior.  0b1 Force ordering. All memory effects seen in the order they are arbitrated.	0b0
[31:30]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[29:28]	UBACCLVL	Access level from the Utility bus.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>7</sup>
[27:25]	RES0	Reserved	RES0
[24]	SCLKQ	SCLK Q-channel operational.  <b>0b0</b> The cluster SCLK Q-channel is permanently active. The SCLKQACTIVE output is always HIGH. Software can use this setting to improve latency in some cases when all cores are in WFx state, or for incoming requests from the ACELS and MACP ports.  <b>0b1</b> The cluster SCLK Q-channel operates normally.	0b1
[23:22]	RES0	Reserved	RES0
[21]	L2EC	Controls the L2 error containment behavior.  <b>0b0</b> This bit has no effect on the L2 error containment behavior.  <b>0b1</b> Blocks all new non-MBIST Main Manager requests when a double-bit ECC error is detected on the L2 tag RAM.	0b0
[20:19]	L2CBLVL	L2 internal CBUSY generation control. Controls the level of activity within the L2 before prefetch throttling is applied.  This field resets to an appropriate value depending on the number of logical cores in the cluster, affected by AArch64-IMP_CLUSTERCFR_EL1.CEMODE: <ul style="list-style-type: none"> <li>When 1 core is present, L2CBLVL resets to 0b00.</li> <li>When 2-7 cores are present, L2CBLVL resets to 0b01.</li> <li>When 8 cores are present, L2CBLVL resets to 0b11.</li> </ul> <b>0b00</b> Feedback is disabled, no prefetch throttling will occur.  <b>0b01</b> Normal thresholds are used, prefetch throttling may occur.  <b>0b10</b> Conservative threshold are used, prefetch throttling may occur earlier than with normal thresholds.  <b>0b11</b> Most conservative thresholds are used, prefetch throttling may occur earlier than with conservative thresholds.	xx

<sup>7</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.



Bits	Name	Description	Reset
[18]	L2DSNPFLT	<b>When CHI == 1</b> L2 downstream snoop filter present. <b>0b0</b> Disables sending Evict transactions when clean cache lines are evicted without data. <b>0b1</b> Enables sending Evict transactions when clean cache lines are evicted without data. <b>Otherwise</b> RES0	'0'
[17]	L2FLUSHEVC	L2 flush evict control. <b>0b0</b> Disables sending data when hardware cache flushes or DC CISC instructions evict a clean cache line. <b>0b1</b> Sending data when hardware cache flushes or DC CISC instructions evict clean cache lines is controlled by L2CDEV. Sending of Evict transactions is controlled by L2DSNPFLT.	0b0
[16:15]	L2PFDFTH	L2 prefetch data forwarding threshold. <b>0b00</b> Default prefetch forwarding behavior. <b>0b01</b> Faster prefetch forwarding timeout. <b>0b10</b> Immediate prefetch forwarding timeout (no waiting). <b>0b11</b> Prefetch forwarding is disabled.	0b00
[14:13]	L2STCTL	L2 cache stashing control. <b>0b00</b> Stashes targeting L2 cache will allocate as if the line were brought in by a load. <b>0b01</b> Stashes targeting L2 cache will allocate and be marked as preferred targets for eviction. <b>0b10</b> Stashes targeting L2 cache will allocate as if the line were brought in by a load, but will only allocate to odd numbered cache ways. <b>0b11</b> Stashes targeting L2 cache will be ignored.	0b00
[12]	L2VFDIS	L2 allocation control for L1 evictions. <b>0b1</b> L1 victims will be allocated to the L2 cache before they can reallocate to L1.	0b1

Bits	Name	Description	Reset
[11:10]	L2CDEVC	<p><b>When CHI == 1</b> L2 cache flushing behavior.</p> <p><b>0b00</b> Disables sending data when clean cache lines are evicted.</p> <p><b>0b01</b> Enables sending WriteEvictFull transactions when Unique Clean cache lines are evicted. Shared Clean cache line evictions do not send data.</p> <p><b>0b10</b> Enables sending WriteEvictOrEvict transactions when Unique Clean cache lines are evicted. Shared Clean cache line evictions do not send data.</p> <p><b>0b11</b> Enables sending WriteEvictOrEvict transactions when Unique Clean or Shared Clean cache lines are evicted.</p> <p><b>Otherwise</b> L2 cache flushing behavior.</p> <p><b>0b00</b> Disables sending data when clean cache lines are evicted.</p> <p><b>0b11</b> Enables sending data when clean cache lines are evicted.</p> <p>All other values are reserved.</p>	'00'
[9]	L2RPUCTL	<p><b>When CHI == 1</b> L2 ReadPreferUnique control.</p> <p><b>0b0</b> ReadPreferUnique will not be sent outside the cluster when core ReadPreferUnique hits SharedClean inside the cluster.</p> <p><b>0b1</b> ReadPreferUnique will be sent outside the cluster when core ReadPreferUnique hits SharedClean inside the cluster.</p> <p><b>Otherwise</b> RES0</p>	'0'
[8]	L2RDLAT	<p>L2 cache Read Latency.</p> <p>This field resets to the value of the L2_DATA_RD_LATENCY global parameter, visible in AArch64-IMP_CLUSTERCFR_EL1.L2RDLAT.</p> <p>This field can be updated by software after a cluster reset, but will only take effect as soon as the L2 cache is idle. Arm recommends that changes are done in periods with low expected activity, for example when the system is booting and before the L2 cache is enabled.</p> <p><b>0b0</b> 2 cycles output delay from L2 data RAMs.</p> <p><b>0b1</b> 3 cycles output delay from L2 data RAMs.</p>	x

Bits	Name	Description	Reset
[7:6]	L2WRLAT	<p>L2 cache Write Latency.</p> <p>This field resets to the value of the L2_DATA_WR_LATENCY global parameter, visible in AArch64-IMP_CLUSTERCFR_EL1.L2WRLAT.</p> <p>This field can be updated by software after a cluster reset, but will only take effect as soon as the L2 cache is idle. Arm recommends that changes are done in periods with low expected activity, for example when the system is booting and before the L2 cache is enabled.</p> <p><b>0b00</b> 1 cycle input delay from L2 data RAMs.</p> <p><b>0b01</b> 2 cycles input delay from L2 data RAMs.</p> <p><b>0b10</b> 2 cycles input delay plus 1 cycle hold from L2 data RAMs.</p>	xx
[5]	L2DDDP	<p>L2 cache stashing snoop disable datapull.</p> <p><b>0b0</b> A stashing snoop will send a datapull request.</p> <p><b>0b1</b> A stashing snoop will not send a datapull request.</p>	0b0
[4]	L2EVADIS	<p>L2 cache POP RAM allocate evict behavior.</p> <p><b>0b0</b> If using POP RAMs, enable the optimized read/write allocate evict mechanism.</p> <p><b>0b1</b> If using POP RAMs, disable the optimized read/write allocate evict mechanism.</p> <p>If the CFGL2EVAIMP configuration pin is 0b0, this bit is <b>RAO/WI</b>.</p>	0b0
[3:2]	L2VIC	<p>L2 Victim control.</p> <p><b>0b00</b> I-side requests use new age of 0b10 (less likely to be evicted).  D-side requests use new age of 0b01 (more likely to be evicted).</p> <p><b>0b01</b> Both i-side and d-side requests use 0b01.</p> <p><b>0b10</b> Both i-side and d-side requests use 0b10.</p> <p><b>0b11</b> Disabled. All ages are treated the same.</p>	0b00
[1]	L2FSM	<p>L2 hazarding optimisation control.</p> <p>Hazarding optimisations will improve average performance but may reduce determinism.</p> <p><b>0b0</b> Hazarding optimisations disabled.</p> <p><b>0b1</b> Hazarding optimisations enabled.</p>	0b1
[0]	RES0	Reserved	RES0

Access

MRS <Xt>, IMP\_CLUSTERACTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b011

MSR IMP\_CLUSTERACTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b011

Accessibility

MRS <Xt>, IMP\_CLUSTERACTLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERACTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERACTLR_EL1;
```

MSR IMP\_CLUSTERACTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.AUX == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERACTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERACTLR_EL1 = X[t, 64];
```

A.2.2.54 IMP\_CLUSTERPWRCTLR\_EL1, Cluster Power Control Register

This register controls power features of the cluster. There is only one IMP\_CLUSTERPWRCTLR\_EL1 register implemented in the cluster, which all cores can access.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-103: AARCH64\_IMP\_CLUSTERPWRCTLR\_EL1 bit assignments

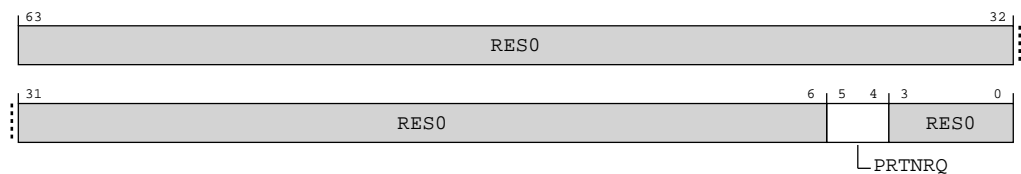


Table A-273: IMP\_CLUSTERPWRCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:6]	RES0	Reserved	RES0
[5:4]	PRTNRQ	<b>When L2_SLICES == 2</b> L2 cache Partition power request. These bits are passed to the PPU as an advisory request for which partitions to power. <b>0b00</b> Request that none of the L2 cache partitions are powered up. <b>0b01</b> Request that half of the L2 cache is powered up. <b>0b11</b> Request that both partitions of the L2 cache are powered up.  <b>Otherwise</b> L2 cache Partition power request. These bits are passed to the PPU as an advisory request for which partitions to power. <b>0b00</b> Request that none of the L2 cache partitions are powered up. <b>0b11</b> Request that both partitions of the L2 cache are powered up.	'11' <sup>8</sup>

<sup>8</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.  
Non-Confidential

Bits	Name	Description	Reset
[3:0]	RES0	Reserved	RES0

### Access

MRS <Xt>, IMP\_CLUSTERPWRCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b101

MSR IMP\_CLUSTERPWRCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b101

### Accessibility

MRS <Xt>, IMP\_CLUSTERPWRCTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPWRCTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPWRCTLR_EL1;

```

MSR IMP\_CLUSTERPWRCTLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.POWER == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPWRCTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPWRCTLR_EL1 = X[t, 64];

```

#### A.2.2.55 IMP\_CLUSTERPWRDN\_EL1, Cluster Power Down Register

This register controls powerdown requirements of the cluster. This register is banked per core, i.e. each core accesses its own copy of the register. Cluster logic combines all registers contents to decide the power strategy.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-104: AARCH64\_IMP\_CLUSTERPWRDN\_EL1 bit assignments

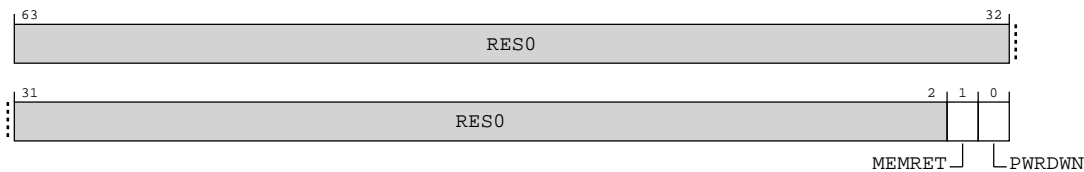


Table A-276: IMP\_CLUSTERPWRDN\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:2]	RES0	Reserved	RES0
[1]	MEMRET	Memory Retention request.  <b>0b0</b> No indication to the PPU.  <b>0b1</b> Indicate to the PPU that memory retention is desired when all cores are powered down. This is an advisory status to the PPU, and will not cause an explicit request to power off the cluster to be denied.	0b0 <sup>9</sup>

<sup>9</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.

Bits	Name	Description	Reset
[0]	PWRDWN	Power Down request.  <b>0b0</b> No indication to the PPU.  <b>0b1</b> Indicate to the PPU that cluster power is required even when all cores are powered down. This is an advisory status to the PPU, and will not cause an explicit request to power off the cluster to be denied.	0b0

### Access

MRS <Xt>, IMP\_CLUSTERPWRDN\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b110

MSR IMP\_CLUSTERPWRDN\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b110

### Accessibility

MRS <Xt>, IMP\_CLUSTERPWRDN\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPWRDN_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPWRDN_EL1;

```

MSR IMP\_CLUSTERPWRDN\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.POWER == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPWRDN_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPWRDN_EL1 = X[t, 64];

```



A.2.2.56 IMP\_CLUSTERPWRSTAT\_EL1, Cluster Power Status Register

This register contains the current status of the cluster power features. There is only one IMP\_CLUSTERPWRSTAT\_EL1 register implemented in the cluster, which all cores can access.

Configurations

This register is available in all configurations.

Attributes

Width

64

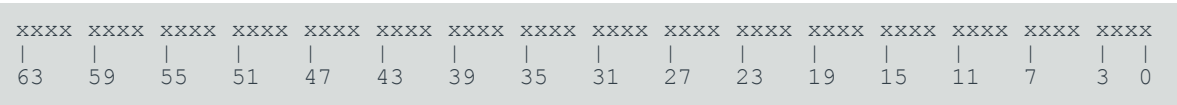
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-105: AARCH64\_IMP\_CLUSTERPWRSTAT\_EL1 bit assignments

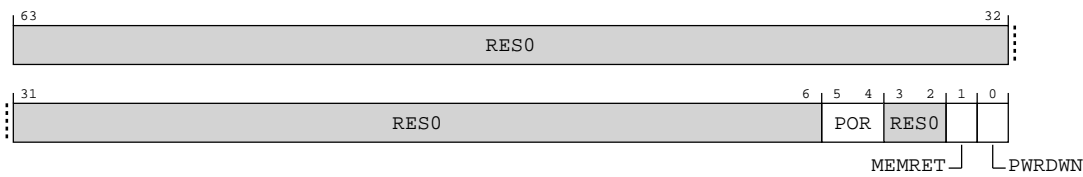


Table A-279: IMP\_CLUSTERPWRSTAT\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:6]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[5:4]	POR	<p><b>When L2_SLICES == 2</b></p> <p>L2 cache Partition power status. This indicates which cache partitions are currently powered up and available. It can be used to determine when the state requested in the AArch64-IMP_CLUSTERPWRCTLR_EL1.PRTNRQ has taken effect.</p> <p><b>0b00</b></p> <p>None of the L2 cache partitions are powered up.</p> <p><b>0b01</b></p> <p>Half of the L2 cache is powered up.</p> <p><b>0b11</b></p> <p>Both partitions of the L2 cache are powered up.</p> <p><b>Otherwise</b></p> <p>L2 cache Partition power status. This indicates which cache partitions are currently powered up and available. It can be used to determine when the state requested in the AArch64-IMP_CLUSTERPWRCTLR_EL1.PRTNRQ has taken effect.</p> <p><b>0b00</b></p> <p>None of the L2 cache partitions are powered up.</p> <p><b>0b11</b></p> <p>Both partitions of the L2 cache are powered up.</p>	xx
[3:2]	RES0	Reserved	RES0
[1]	MEMRET	<p>Memory retention enabled. This bit is a combined version of all banked per-thread bits from the AArch64-IMP_CLUSTERPWRDN_EL1 register.</p> <p><b>0b0</b></p> <p>Memory retention inactive.</p> <p><b>0b1</b></p> <p>Memory retention enabled when all cores powered down.</p>	x
[0]	PWRDWN	<p>Disabled cluster power down. Note this bit is a combined version of all banked per-thread bits from the AArch64-IMP_CLUSTERPWRDN_EL1 register.</p> <p><b>0b0</b></p> <p>Cluster power down active.</p> <p><b>0b1</b></p> <p>Cluster power down disabled when all cores powered down.</p>	x

## Access

MRS <Xt>, IMP\_CLUSTERPWRSTAT\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0011	0b111

## Accessibility

MRS <Xt>, IMP\_CLUSTERPWRSTAT\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPWRSTAT_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPWRSTAT_EL1;
```

A.2.2.57 IMP\_CLUSTERSID\_EL1, Cluster Scheme ID Register

This register controls the L2 cache partitioning Scheme ID for a core. The register is banked per core, i.e. each core accesses its own copy of the register.

Configurations

This register is available in all configurations.

Attributes

Width

64

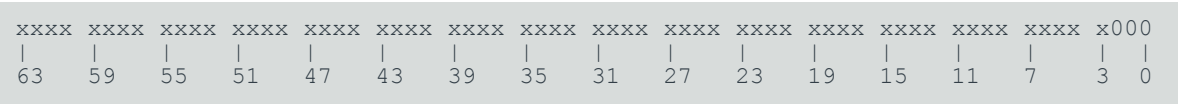
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-106: AARCH64\_IMP\_CLUSTERSID\_EL1 bit assignments

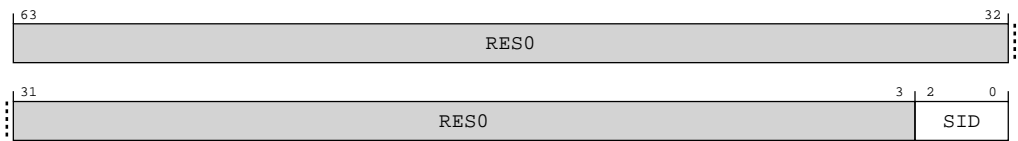


Table A-281: IMP\_CLUSTERSID\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2:0]	SID	Scheme ID. Selects one of the 8 available L2 cache scheme IDs. Memory accesses from this core which reach the L2 cache will use the scheme ID specified by the SID field, as defined by the AArch64-IMP_CLUSTERPARTCR_EL1 register.	0b000

### Access

MRS <Xt>, IMP\_CLUSTERSID\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b000

MSR IMP\_CLUSTERSID\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b000

### Accessibility

MRS <Xt>, IMP\_CLUSTERSID\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERSID_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERSID_EL1;

```

MSR IMP\_CLUSTERSID\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPORTS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERSID_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_CLUSTERSID_EL1 = X[t, 64];

```

## A.2.2.58 IMP\_CLUSTERACPSID\_EL1, Cluster ACP Scheme ID Register

This register controls the L2 cache partitioning Scheme IDs for ACP accesses and Stash requests.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000	x000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-107: AARCH64\_IMP\_CLUSTERACPSID\_EL1 bit assignments

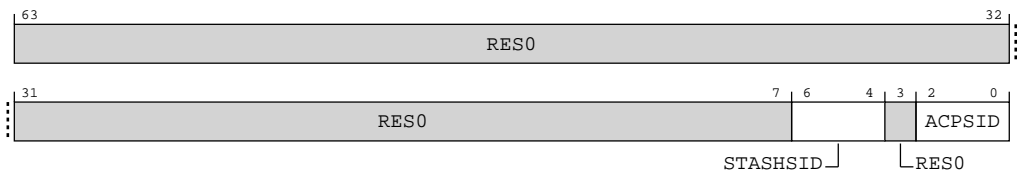


Table A-284: IMP\_CLUSTERACPSID\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:7]	RES0	Reserved	RES0
[6:4]	STASHSID	Stash Scheme ID. Selects one of the 8 available L2 cache scheme IDs. Stash requests from the MM port (when using CHI) which reach the L2 cache will use the scheme ID specified by the STASHID field, as defined by the AArch64-IMP_CLUSTERPARTCR_EL1 register. This field has no effect when CHI is not implemented.	0b000
[3]	RES0	Reserved	RES0
[2:0]	ACPSID	ACP Scheme ID. Selects one of the 8 available L2 cache scheme IDs. Accesses from the MACP port which reach the L2 cache will use the scheme ID specified by the ACPSID field, as defined by the AArch64-IMP_CLUSTERPARTCR_EL1 register.	0b000

Access

MRS <Xt>, IMP\_CLUSTERACPSID\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b001

MSR IMP\_CLUSTERACPSID\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b001

Accessibility

MRS <Xt>, IMP\_CLUSTERACPSID\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERACPSID_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERACPSID_EL1;
```

MSR IMP\_CLUSTERACPSID\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPORTS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERACPSID_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERACPSID_EL1 = X[t, 64];
```

A.2.2.59 IMP\_CLUSTERPARTCR\_EL1, Cluster Partition Control Register

This register controls the L2 cache partitioning. It defines how the 4 way groups map onto the 8 Scheme IDs.

Configurations

This register is available in all configurations.

Attributes

Width

64

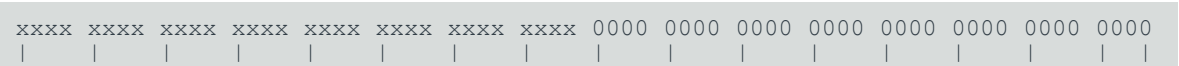
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



63 59 55 51 47 43 39 35 31 27 23 19 15 11 7 3 0

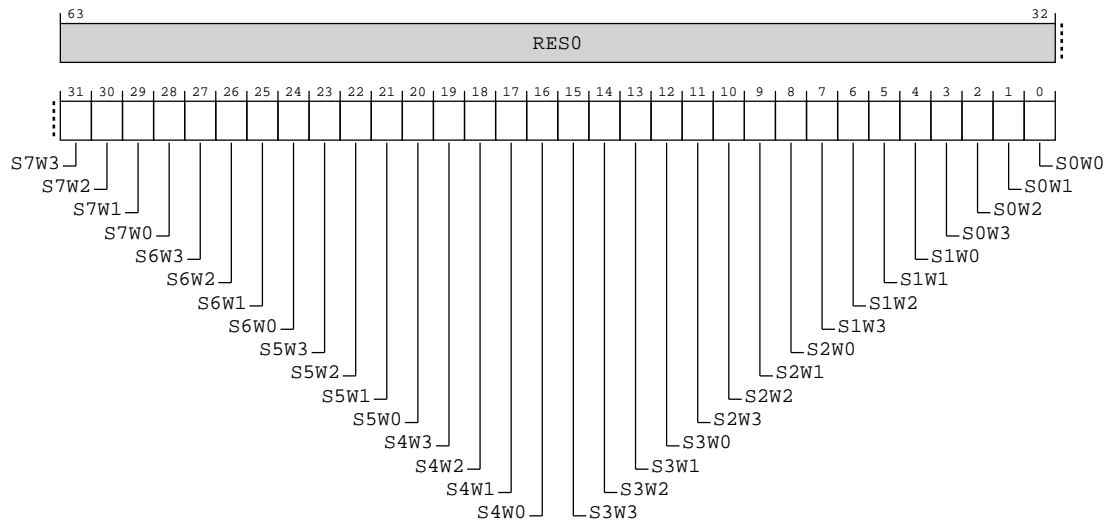


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-108: AARCH64\_IMP\_CLUSTERPARTCR\_EL1 bit assignments**



**Table A-287: IMP\_CLUSTERPARTCR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	S7W3	L2 Cache Way Group 3 mapping to Scheme ID 7. <b>0b0</b> Way Group 3 not assigned to Scheme ID 7. <b>0b1</b> Way Group 3 assigned to Scheme ID 7.	0b0
[30]	S7W2	L2 Cache Way Group 2 mapping to Scheme ID 7. <b>0b0</b> Way Group 2 not assigned to Scheme ID 7. <b>0b1</b> Way Group 2 assigned to Scheme ID 7.	0b0
[29]	S7W1	L2 Cache Way Group 1 mapping to Scheme ID 7. <b>0b0</b> Way Group 1 not assigned to Scheme ID 7. <b>0b1</b> Way Group 1 assigned to Scheme ID 7.	0b0

Bits	Name	Description	Reset
[28]	S7W0	L2 Cache Way Group 0 mapping to Scheme ID 7. <b>0b0</b> Way Group 0 not assigned to Scheme ID 7. <b>0b1</b> Way Group 0 assigned to Scheme ID 7.	0b0
[27]	S6W3	L2 Cache Way Group 3 mapping to Scheme ID 6. <b>0b0</b> Way Group 3 not assigned to Scheme ID 6. <b>0b1</b> Way Group 3 assigned to Scheme ID 6.	0b0
[26]	S6W2	L2 Cache Way Group 2 mapping to Scheme ID 6. <b>0b0</b> Way Group 2 not assigned to Scheme ID 6. <b>0b1</b> Way Group 2 assigned to Scheme ID 6.	0b0
[25]	S6W1	L2 Cache Way Group 1 mapping to Scheme ID 6. <b>0b0</b> Way Group 1 not assigned to Scheme ID 6. <b>0b1</b> Way Group 1 assigned to Scheme ID 6.	0b0
[24]	S6W0	L2 Cache Way Group 0 mapping to Scheme ID 6. <b>0b0</b> Way Group 0 not assigned to Scheme ID 6. <b>0b1</b> Way Group 0 assigned to Scheme ID 6.	0b0
[23]	S5W3	L2 Cache Way Group 3 mapping to Scheme ID 5. <b>0b0</b> Way Group 3 not assigned to Scheme ID 5. <b>0b1</b> Way Group 3 assigned to Scheme ID 5.	0b0
[22]	S5W2	L2 Cache Way Group 2 mapping to Scheme ID 5. <b>0b0</b> Way Group 2 not assigned to Scheme ID 5. <b>0b1</b> Way Group 2 assigned to Scheme ID 5.	0b0
[21]	S5W1	L2 Cache Way Group 1 mapping to Scheme ID 5. <b>0b0</b> Way Group 1 not assigned to Scheme ID 5. <b>0b1</b> Way Group 1 assigned to Scheme ID 5.	0b0



Bits	Name	Description	Reset
[20]	S5W0	L2 Cache Way Group 0 mapping to Scheme ID 5. <b>0b0</b> Way Group 0 not assigned to Scheme ID 5. <b>0b1</b> Way Group 0 assigned to Scheme ID 5.	0b0
[19]	S4W3	L2 Cache Way Group 3 mapping to Scheme ID 4. <b>0b0</b> Way Group 3 not assigned to Scheme ID 4. <b>0b1</b> Way Group 3 assigned to Scheme ID 4.	0b0
[18]	S4W2	L2 Cache Way Group 2 mapping to Scheme ID 4. <b>0b0</b> Way Group 2 not assigned to Scheme ID 4. <b>0b1</b> Way Group 2 assigned to Scheme ID 4.	0b0
[17]	S4W1	L2 Cache Way Group 1 mapping to Scheme ID 4. <b>0b0</b> Way Group 1 not assigned to Scheme ID 4. <b>0b1</b> Way Group 1 assigned to Scheme ID 4.	0b0
[16]	S4W0	L2 Cache Way Group 0 mapping to Scheme ID 4. <b>0b0</b> Way Group 0 not assigned to Scheme ID 4. <b>0b1</b> Way Group 0 assigned to Scheme ID 4.	0b0
[15]	S3W3	L2 Cache Way Group 3 mapping to Scheme ID 3. <b>0b0</b> Way Group 3 not assigned to Scheme ID 3. <b>0b1</b> Way Group 3 assigned to Scheme ID 3.	0b0
[14]	S3W2	L2 Cache Way Group 2 mapping to Scheme ID 3. <b>0b0</b> Way Group 2 not assigned to Scheme ID 3. <b>0b1</b> Way Group 2 assigned to Scheme ID 3.	0b0
[13]	S3W1	L2 Cache Way Group 1 mapping to Scheme ID 3. <b>0b0</b> Way Group 1 not assigned to Scheme ID 3. <b>0b1</b> Way Group 1 assigned to Scheme ID 3.	0b0

Bits	Name	Description	Reset
[12]	S3W0	L2 Cache Way Group 0 mapping to Scheme ID 3. <b>0b0</b> Way Group 0 not assigned to Scheme ID 3. <b>0b1</b> Way Group 0 assigned to Scheme ID 3.	0b0
[11]	S2W3	L2 Cache Way Group 3 mapping to Scheme ID 2. <b>0b0</b> Way Group 3 not assigned to Scheme ID 2. <b>0b1</b> Way Group 3 assigned to Scheme ID 2.	0b0
[10]	S2W2	L2 Cache Way Group 2 mapping to Scheme ID 2. <b>0b0</b> Way Group 2 not assigned to Scheme ID 2. <b>0b1</b> Way Group 2 assigned to Scheme ID 2.	0b0
[9]	S2W1	L2 Cache Way Group 1 mapping to Scheme ID 2. <b>0b0</b> Way Group 1 not assigned to Scheme ID 2. <b>0b1</b> Way Group 1 assigned to Scheme ID 2.	0b0
[8]	S2W0	L2 Cache Way Group 0 mapping to Scheme ID 2. <b>0b0</b> Way Group 0 not assigned to Scheme ID 2. <b>0b1</b> Way Group 0 assigned to Scheme ID 2.	0b0
[7]	S1W3	L2 Cache Way Group 3 mapping to Scheme ID 1. <b>0b0</b> Way Group 3 not assigned to Scheme ID 1. <b>0b1</b> Way Group 3 assigned to Scheme ID 1.	0b0
[6]	S1W2	L2 Cache Way Group 2 mapping to Scheme ID 1. <b>0b0</b> Way Group 2 not assigned to Scheme ID 1. <b>0b1</b> Way Group 2 assigned to Scheme ID 1.	0b0
[5]	S1W1	L2 Cache Way Group 1 mapping to Scheme ID 1. <b>0b0</b> Way Group 1 not assigned to Scheme ID 1. <b>0b1</b> Way Group 1 assigned to Scheme ID 1.	0b0

Bits	Name	Description	Reset
[4]	S1W0	L2 Cache Way Group 0 mapping to Scheme ID 1.  <b>0b0</b> Way Group 0 not assigned to Scheme ID 1.  <b>0b1</b> Way Group 0 assigned to Scheme ID 1.	0b0
[3]	S0W3	L2 Cache Way Group 3 mapping to Scheme ID 0.  <b>0b0</b> Way Group 3 not assigned to Scheme ID 0.  <b>0b1</b> Way Group 3 assigned to Scheme ID 0.	0b0
[2]	S0W2	L2 Cache Way Group 2 mapping to Scheme ID 0.  <b>0b0</b> Way Group 2 not assigned to Scheme ID 0.  <b>0b1</b> Way Group 2 assigned to Scheme ID 0.	0b0
[1]	S0W1	L2 Cache Way Group 1 mapping to Scheme ID 0.  <b>0b0</b> Way Group 1 not assigned to Scheme ID 0.  <b>0b1</b> Way Group 1 assigned to Scheme ID 0.	0b0
[0]	S0W0	L2 Cache Way Group 0 mapping to Scheme ID 0.  <b>0b0</b> Way Group 0 not assigned to Scheme ID 0.  <b>0b1</b> Way Group 0 assigned to Scheme ID 0.	0b0

## Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPARTCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b011

MSR IMP\_CLUSTERPARTCR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b011

## Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERPARTCR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then

```

```
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPARTCR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERPARTCR_EL1;
```

MSR IMP\_CLUSTERPARTCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPORTS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPARTCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_CLUSTERPARTCR_EL1 = X[t, 64];
```

A.2.2.60 IMP\_CLUSTERQOSR\_EL1, Cluster Quality of Service Register

This register controls the Quality of Service aspects for the cluster.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0xxx	1110
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-109: AARCH64\_IMP\_CLUSTERQOSR\_EL1 bit assignments

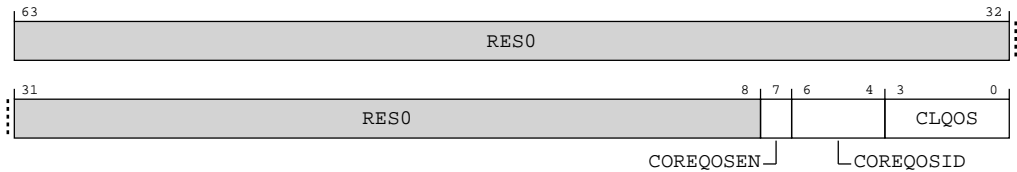


Table A-290: IMP\_CLUSTERQOSR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7]	COREQOSEN	Quality of Service enable within the cluster.  <b>0b0</b> Quality of Service disabled within the cluster. The LCU and the L2 cache arbitrate core requests fairly.  <b>0b1</b> Quality of Service enabled within the cluster. The LCU and the L2 cache arbitrate requests from core COREQOSID with higher priority than to other cores.	0b0
[6:4]	COREQOSID	Core ID to get higher priority. This field has no effect when COREQOSEN is low.	xxx
[3:0]	CLQOS	Quality of Service setting for the whole cluster. This value will be driven on the Main Manager QoS signals.	0b1110

Access

MRS <Xt>, IMP\_CLUSTERQOSR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b100

MSR IMP\_CLUSTERQOSR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b100

Accessibility

MRS <Xt>, IMP\_CLUSTERQOSR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERQOSR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERQOSR_EL1;
```

MSR IMP\_CLUSTERQOSR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPORTS == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERQOSR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERQOSR_EL1 = X[t, 64];
```

A.2.2.61 IMP\_CLUSTERACELSCTLR\_EL1, ACELS Port Control Register

This register controls the accesses from the ACELS port.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx11	1111	1111	1111	1111
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-110: AARCH64\_IMP\_CLUSTERACELSTLR\_EL1 bit assignments

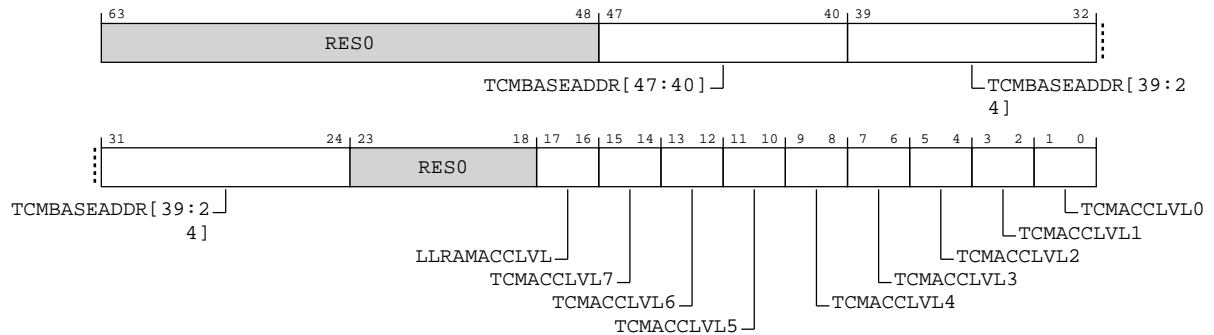


Table A-293: IMP\_CLUSTERACELSTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:40]	TCMBASEADDR[47:40]	<b>When PA_W == 48</b> TCMBs base address as seen from the ACELS port, bits [47:40]. This field is read-only. This field takes the value of the CFGACELSTCMBASEADDR[47:40] configuration pins.  <b>Otherwise</b> RES0	8 {x}
[39:24]	TCMBASEADDR[39:24]	TCMBs base address as seen from the ACELS port, bits [39:24] (aligned to 16 MB). This field takes the value of the CFGACELSTCMBASEADDR[39:24] configuration pins.  <b>Note:</b> There is only one CFGACELSTCMBASEADDR address for the whole processor. Each core's TCM memory is accessible at an offset from this address: <ul style="list-style-type: none"> <li>Core #0 ITCM: offset 0x0</li> <li>Core #0 DTCM: offset 0x10_0000 (1 MiB)</li> <li>Core #1 ITCM: offset 0x20_0000 (2 MiB)</li> <li>Core #1 DTCM: offset 0x30_0000 (3 MiB)</li> <li>...</li> <li>Core #7 ITCM: offset 0xE0_0000 (14 MiB)</li> <li>Core #7 DTCM: offset 0xF0_0000 (15 MiB)</li> </ul> Access to this field is: RO	16 {x}
[23:18]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[17:16]	LLRAMACCLVL	LLRAM access level from the ACELS port.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>10</sup>
[15:14]	TCMACCLVL7	TCM access level from the ACELS port for CPU 7.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>11</sup>
[13:12]	TCMACCLVL6	TCM access level from the ACELS port for CPU 6.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>12</sup>
[11:10]	TCMACCLVL5	TCM access level from the ACELS port for CPU 5.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>13</sup>

<sup>10</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>11</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>12</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>13</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.



Bits	Name	Description	Reset
[9:8]	TCMACCLVL4	TCM access level from the ACELS port for CPU 4.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>14</sup>
[7:6]	TCMACCLVL3	TCM access level from the ACELS port for CPU 3.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>15</sup>
[5:4]	TCMACCLVL2	TCM access level from the ACELS port for CPU 2.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>16</sup>
[3:2]	TCMACCLVL1	TCM access level from the ACELS port for CPU 1.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>17</sup>

<sup>14</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>15</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>16</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.<sup>17</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.

Bits	Name	Description	Reset
[1:0]	TCMACCLVLO	TCM access level from the ACELS port for CPU 0.  <b>0b00</b> No accesses allowed.  <b>0b01</b> Privileged accesses only allowed.  <b>0b11</b> Privileged and unprivileged accesses allowed.  Other values are Reserved.	0b11 <sup>18</sup>

## Access

After a write to AArch64-IMP\_CLUSTERACELSTLR\_EL1, the programmed permission change will only take effect after there are no new transactions on a given channel. A stream of transactions will use the old permissions until there is an idle cycle and then subsequent transactions will use the new permissions.

MRS <Xt>, IMP\_CLUSTERACELSTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b101

MSR IMP\_CLUSTERACELSTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b101

## Accessibility

After a write to AArch64-IMP\_CLUSTERACELSTLR\_EL1, the programmed permission change will only take effect after there are no new transactions on a given channel. A stream of transactions will use the old permissions until there is an idle cycle and then subsequent transactions will use the new permissions.

MRS <Xt>, IMP\_CLUSTERACELSTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERACELSTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERACELSTLR_EL1;

```

MSR IMP\_CLUSTERACELSTLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then

```

<sup>18</sup> This field is preserved on a reset when exiting either MEM\_RET or MEM\_RET\_EMU mode.

```
    UNDEFINED;
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPORTS == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            IMP_CLUSTERACELSTCLR_EL1 = X[t, 64];
        elsif PSTATE.EL == EL2 then
            IMP_CLUSTERACELSTCLR_EL1 = X[t, 64];
```

### A.2.2.62 IMP\_CLUSTERMEMPROTCTLR\_EL1, Cluster Memory Protection Control Register

This register controls the memory protection and bus protection features of the cluster.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic System Control

##### Access type

See bit descriptions

##### Reset value

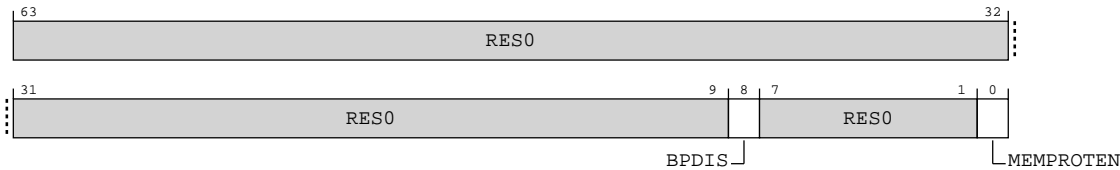
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-111: AARCH64\_IMP\_CLUSTERMEMPROTCTLR\_EL1 bit assignments



**Table A-296: IMP\_CLUSTERMEMPROTCTLR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:9]	RES0	Reserved	RES0
[8]	BPDIS	Bus protection error logging disable.  <b>0b0</b> Bus protection error logging enabled.  <b>0b1</b> Bus protection error logging disabled.	0b0
[7:1]	RES0	Reserved	RES0
[0]	MEMPROTEN	Memory protection enable.  <b>0b0</b> Structures required to support internal RAM protection functionality are turned off.  <b>0b1</b> Structures required to support internal RAM protection functionality are turned on.  <ul style="list-style-type: none"> <li>This field must not be programmed while the caches are enabled, otherwise the behavior of the processor memory system becomes <b>UNPREDICTABLE</b>. Software must ensure that the processor caches are disabled before programming this field. After programming this field, software must ensure that the caches are invalidated before they can be enabled again.</li> <li>If the values of AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN for all cores in the processor cluster are not the same, it is possible for wrong data values to be consumed by any core in the cluster, because errors that are locally suppressed by disabling RAM protection may spread through hardware data coherency mechanisms. Arm recommends that AArch64-IMP_CLUSTERMEMPROTCTLR_EL1.MEMPROTEN and all AArch64-IMP_MEMPROTCTLR_EL1.MEMPROTEN fields are programmed with the same value, unless otherwise directed by Arm.</li> </ul>	x

### Access

MRS &lt;Xt&gt;, IMP\_CLUSTERMEMPROTCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b110

MSR IMP\_CLUSTERMEMPROTCTLR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0100	0b110

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERMEMPROTCTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERMEMPROTCTLR_EL1;
    elsif PSTATE.EL == EL2 then

```

```
X[t, 64] = IMP_CLUSTERMEMPROTCTLR_EL1;
```

MSR IMP\_CLUSTERMEMPROTCTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.DIAGNOSTIC == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERMEMPROTCTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERMEMPROTCTLR_EL1 = X[t, 64];
```

A.2.2.63 AIDR\_EL1, Auxiliary ID Register

Provides **IMPLEMENTATION DEFINED** identification information.

The value of this register must be interpreted in conjunction with the value of AArch64-MIDR\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-112: AARCH64\_AIDR\_EL1 bit assignments

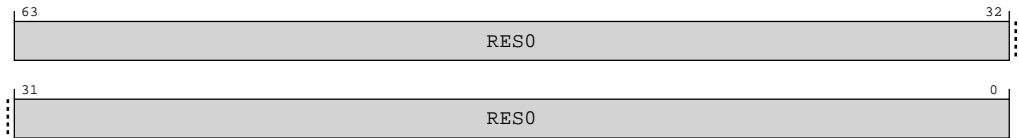


Table A-299: AIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, AIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b001	0b0000	0b0000	0b111

Accessibility

MRS <Xt>, AIDR\_EL1

```
if PSTATE.EL == EL0 then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TID1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = AIDR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = AIDR_EL1;
```

A.2.2.64 IMP\_CDBGDR0\_EL1, Cache Debug Data Register 0

Contains data from a preceeding cache debug operation.

This register is populated after one of the following operations have been executed:

- SYS IMP\_CDBGDCD
- SYS IMP\_CDBGDCT
- SYS IMP\_CDBGICD
- SYS IMP\_CDBGICT
- SYS IMP\_CDBGTD
- SYS IMP\_CDBGTT

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

When the last cache debug operation was SYS IMP\_CDBGDCD, or the last cache debug operation was SYS IMP\_CDBGICD or the last cache debug operation was SYS IMP\_CDBGDTD

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGDCT

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGICT

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGTD and index is in range 0x000 - 0xFF

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGTD and index is in range 0x100 - 0x107

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGTT and index is in range 0x000 - 0xFF

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CDBGTT and index is in range 0x100 - 0x107

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

When the last cache debug operation was SYS IMP\_CDBGDCD, or the last cache debug operation was SYS IMP\_CDBGICD or the last cache debug operation was SYS IMP\_CBGDTD

Figure A-113: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments

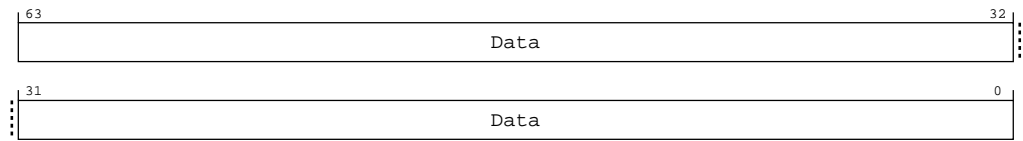


Table A-301: IMP\_CDBGDR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	Data	Data contents of cache at specified Set/Way/Offset	64 { x }

When the last cache debug operation was SYS IMP\_CDBGDCT

Figure A-114: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments

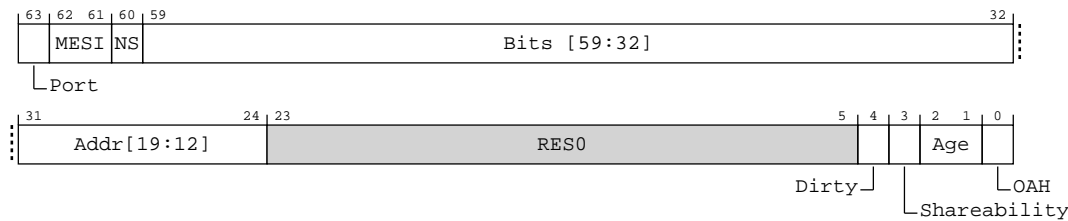


Table A-302: IMP\_CDBGDR0\_EL1 bit descriptions

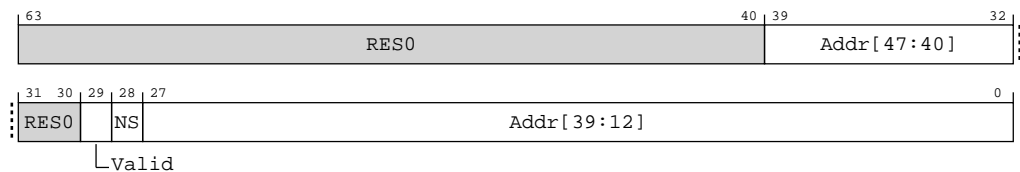
Bits	Name	Description	Reset
[63]	Port	Port (from Tag contents, not stored in RAM)  <b>0b0</b> Main Manager port  <b>0b1</b> LLRAM port	x
[62:61]	MESI	MESI State (from Tag RAM)  <b>0b00</b> Invalid  <b>0b01</b> Shared  <b>0b10</b> Unique  <b>0b11</b> Unique (Transient)	xx
[60]	NS	Non-secure state (from Tag RAM)	x



Bits	Name	Description	Reset
[59:32]	Addr[47:20]	<b>When PA_W == 48</b> Tag Address, Physical Address [47:20] (from Tag RAM).  <b>Otherwise</b> Tag Address, Physical Address [39:12] (from Tag RAM).	28 {x}
[31:24]	Addr[19:12]	<b>When PA_W == 48</b> Tag Address, Physical Address [19:12] (from Tag RAM).  <b>Otherwise</b> RES0	8 {x}
[23:5]	RES0	Reserved	RES0
[4]	Dirty	Dirty bit (from Dirty RAM)  <b>0b0</b> Clean  <b>0b1</b> Modified/Dirty	x
[3]	Shareability	Shareability (from Dirty RAM)	x
[2:1]	Age	Age (from Dirty RAM)	xx
[0]	OAH	Outer Allocation Hint (from Dirty RAM)	x

When the last cache debug operation was SYS IMP\_CDBGICT

**Figure A-115: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments**



**Table A-303: IMP\_CDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	Addr[47:40]	<b>When PA_W == 48</b> Tag Address, Physical Address [47:40] (from Tag RAM).  <b>Otherwise</b> RES0	8 {x}
[31:30]	RES0	Reserved	RES0
[29]	Valid	Valid	x
[28]	NS	Non-secure state	x
[27:0]	Addr[39:12]	Tag Address, Physical Address [39:12]	28 {x}

When the last cache debug operation was SYS IMP\_CDBGTD and index is in range 0x0000x0FF

Figure A-116: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments

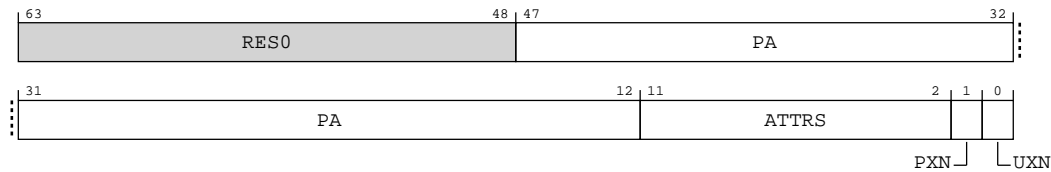


Table A-304: IMP\_CDBGDR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:12]	PA	The Physical Address.	36{x}
[11:2]	ATTRS	Defines the memory attribute.	10{x}
[1]	PXN	Executable in stage 1 non-user mode.	x
[0]	UXN	Executable in stage 1 user mode.	x

When the last cache debug operation was SYS IMP\_CDBGTD and index is in range 0x1000x107

Figure A-117: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments

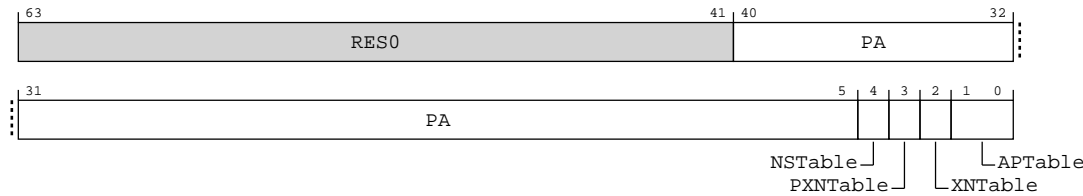
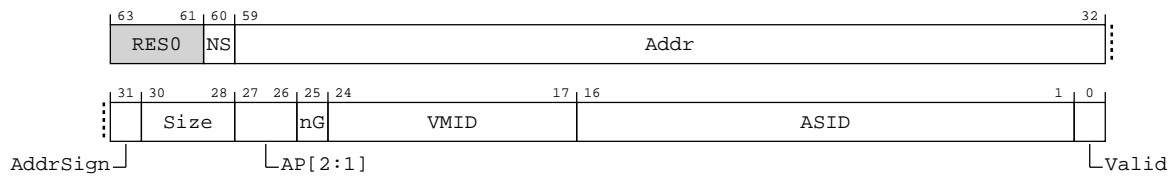


Table A-305: IMP\_CDBGDR0\_EL1 bit descriptions

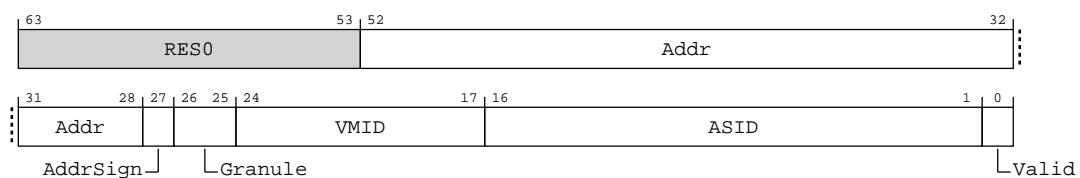
Bits	Name	Description	Reset
[63:41]	RES0	Reserved	RES0
[40:5]	PA	The physical base address of L3 descriptor.  <b>Note:</b> This is the actual physical address, but a stage 2 lookup will still be required to obtain the combined attributes.	36{x}
[4]	NSTable	Combined NSTable bits from stage 1 descriptors up to last level.	x
[3]	PXNTable	Stores the stage 1 privilege execution permission information up to last level, starts from executable (0b0) and combined with PXNTable bits from stage 1 descriptors up to last level.	x
[2]	XNTable	Stores the stage 1 execution permission information up to last level, starts from executable (0b0) and combined with XNTable bits from stage 1 descriptors up to last level.	x
[1:0]	APTable	Stores the stage 1 access permission information up to last level, starts from full access (0b01) and combined with APTTable bits from stage 1 descriptors up to last level.	xx

When the last cache debug operation was SYS IMP\_CDBGTT and index is in range 0x0000x0FF

**Figure A-118: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments****Table A-306: IMP\_CDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:61]	RES0	Reserved	RES0
[60]	NS	The security state allocated to this memory region.	x
[59:32]	Addr	Virtual Address. Depending on the page size, unused lower bits are 0.	28 {x}
[31]	AddrSign	The Virtual Address Sign bit, VA[48].	x
[30:28]	Size	Page or block size of the stage 1 translation result.	xxx
[27:26]	AP[2:1]	Data Access Permissions bits.	xx
[25]	nG	The not global bit.	x
[24:17]	VMID	Virtual machine identifier.	8 {x}
[16:1]	ASID	Address space identifier. This field will be 0 if ASID is not used.	16 {x}
[0]	Valid	Valid	x

When the last cache debug operation was SYS IMP\_CDBGTT and index is in range 0x1000x107

**Figure A-119: AARCH64\_IMP\_CDBGDR0\_EL1 bit assignments****Table A-307: IMP\_CDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:53]	RES0	Reserved	RES0
[52:28]	Addr	Virtual Address. Depending on the page size, unused lower bits are 0.	25 {x}
[27]	AddrSign	The Virtual Address Sign bit, VA[48].	x
[26:25]	Granule	Translation granule size.	xx
[24:17]	VMID	Virtual machine identifier.	8 {x}
[16:1]	ASID	Address space identifier.	16 {x}
[0]	Valid	Valid	x

## Access

MRS <Xt>, IMP\_CDBGDR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b0000	0b000

Accessibility

MRS <Xt>, IMP\_CDBGDR0\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CDBGDR0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CDBGDR0_EL1;
```

A.2.2.65 IMP\_CDBGDR1\_EL1, Cache Debug Data Register 1

Contains data from a preceeding cache debug operation.

This register is populated or zeroed after one of the following operations have been executed:

- SYS IMP\_CDBGDCD
- SYS IMP\_CDBGDCT
- SYS IMP\_CDBGICD
- SYS IMP\_CDBGICT
- SYS IMP\_CDBGTD
- SYS IMP\_CDBGTT

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-120: AARCH64\_IMP\_CDBGDR1\_EL1 bit assignments

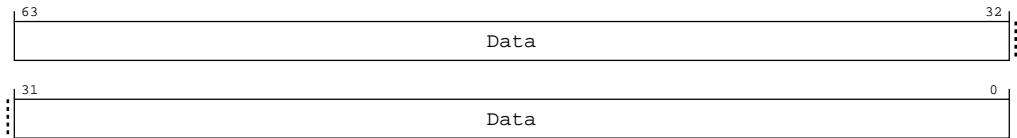


Table A-309: IMP\_CDBGDR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	Data	Data contents of cache at specified Set/Way/Offset	64 { x }

Access

MRS <Xt>, IMP\_CDBGDR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b0000	0b001

Accessibility

MRS <Xt>, IMP\_CDBGDR1\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CDBGDR1_EL1;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CDBGDR1_EL1;
```

A.2.2.66 IMP\_CLUSTERCDBGDR0\_EL1, Cluster Cache Debug Data Register 0

Contains data from a preceeding cache debug operation.

This register is populated after one of the following operations have been executed:

- SYS IMP\_CLUSTERCDBGL2D
- SYS IMP\_CLUSTERCDBGL2T
- SYS IMP\_CLUSTERCDBGL2DT

- SYS IMP\_CLUSTERCDBGLCUdT

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2D

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2T and PA\_W == 40

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2T and PA\_W == 48

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2DT and PA\_W == 40

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2DT and PA\_W == 48

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When the last cache debug operation was SYS IMP\_CLUSTERCDBGLCUdT

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

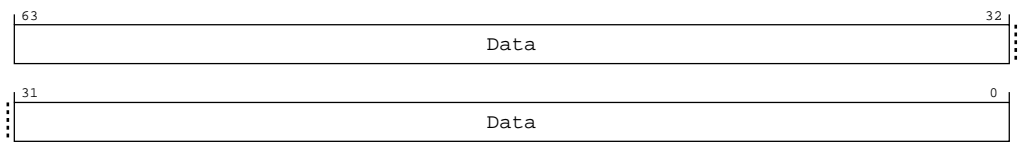


Where the reset reads xxxx, see individual bits.

Bit descriptions

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2D

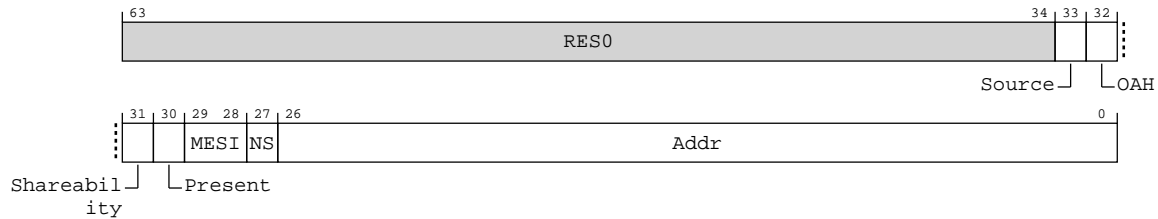
Figure A-121: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments



**Table A-311: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions**

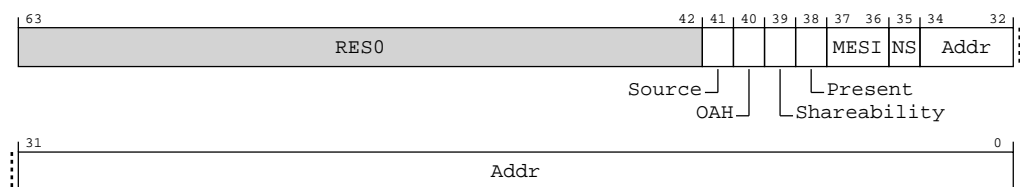
Bits	Name	Description	Reset
[63:0]	Data	Data contents of cache at specified Set/Way/Offset	64 {x}

When the last cache debug operation was SYS IMP\_CLUSTERCDBGDL2T and PA\_W == 40

**Figure A-122: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments****Table A-312: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:34]	RES0	Reserved	RES0
[33]	Source	Cache line source	x
[32]	OAH	Outer Allocation Hint (from Dirty RAM)	x
[31]	Shareability	Shareability (from Dirty RAM)	x
[30]	Present	Cache line is present in the L1 cache of any of the cores in this cluster.	x
[29:28]	MESI	MESI State (from Tag RAM)  0b00 Invalid 0b01 Shared Clean 0b10 Unique Dirty 0b11 Unique Clean	xx
[27]	NS	Non-secure state (from Tag RAM)	x
[26:0]	Addr	Tag Address, Physical Address [39:12] (from Tag RAM)	27 {x}

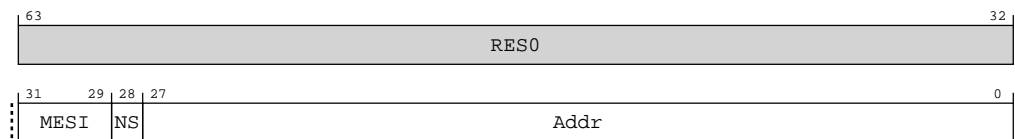
When the last cache debug operation was SYS IMP\_CLUSTERCDBGDL2T and PA\_W == 48

**Figure A-123: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments**

**Table A-313: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:42]	RES0	Reserved	RES0
[41]	Source	Cache line source	x
[40]	OAH	Outer Allocation Hint (from Dirty RAM)	x
[39]	Shareability	Shareability (from Dirty RAM)	x
[38]	Present	Cache line is present in the L1 cache of any of the cores in this cluster.	x
[37:36]	MESI	MESI State (from Tag RAM)  <b>0b00</b> Invalid  <b>0b01</b> Shared Clean  <b>0b10</b> Unique Dirty  <b>0b11</b> Unique Clean	xx
[35]	NS	Non-secure state (from Tag RAM)	x
[34:0]	Addr	Tag Address, Physical Address [47:12] (from Tag RAM)	35 {x}

When the last cache debug operation was SYS IMP\_CLUSTERCDBGDL2DT and PA\_W == 40

**Figure A-124: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments****Table A-314: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[31:29]	MESI	MESI State (from Tag RAM)  <b>0b000</b> Invalid  <b>0b001</b> Cluster unique, CPU shared clean, non-shareable  <b>0b010</b> Cluster unique, CPU shared dirty, non-shareable  <b>0b011</b> Cluster unique, CPU unique, non-shareable  <b>0b100</b> Cluster unique, CPU shared clean, shareable  <b>0b101</b> Cluster unique, CPU shared dirty, shareable  <b>0b110</b> Cluster unique, CPU unique, shareable  <b>0b111</b> Cluster shared, CPU shared, shareable	xxx
[28]	NS	Non-secure state (from Tag RAM)	x
[27:0]	Addr	Tag Address, Physical Address [39:12] (from Tag RAM)	28 {x}

When the last cache debug operation was SYS IMP\_CLUSTERCDBGL2DT and PA\_W == 48

Figure A-125: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments

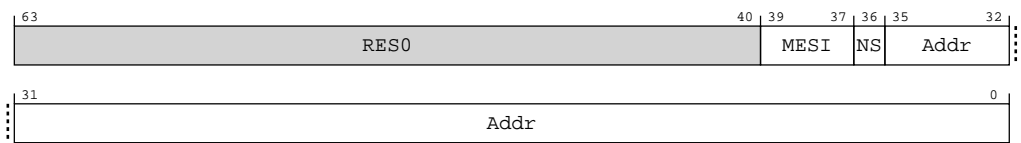


Table A-315: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[39:37]	MESI	MESI State (from Tag RAM)  <b>0b000</b> Invalid  <b>0b001</b> Cluster unique, CPU shared clean, non-shareable  <b>0b010</b> Cluster unique, CPU shared dirty, non-shareable  <b>0b011</b> Cluster unique, CPU unique, non-shareable  <b>0b100</b> Cluster unique, CPU shared clean, shareable  <b>0b101</b> Cluster unique, CPU shared dirty, shareable  <b>0b110</b> Cluster unique, CPU unique, shareable  <b>0b111</b> Cluster shared, CPU shared, shareable	xxx
[36]	NS	Non-secure state (from Tag RAM)	x
[35:0]	Addr	Tag Address, Physical Address [47:12] (from Tag RAM)	36{x}

When the last cache debug operation was SYS IMP\_CLUSTERCDBGDGLCUdT

Figure A-126: AARCH64\_IMP\_CLUSTERCDBGDR0\_EL1 bit assignments

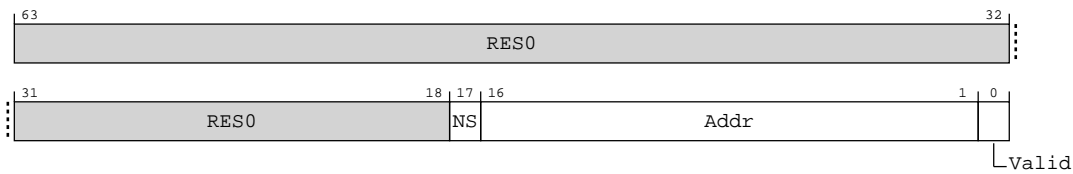


Table A-316: IMP\_CLUSTERCDBGDR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:18]	RES0	Reserved	RES0
[17]	NS	Non-secure state (from Tag RAM)	x
[16:1]	Addr	Tag Address (from Tag RAM)  The tag width depends on the implemented cache size. The unused bits are <b>RES0</b> . The LLRAM base address is excluded from the stored address bits.	16{x}
[0]	Valid	Valid	x

Access

MRS <Xt>, IMP\_CLUSTERCDBGDR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b0011	0b000

## Accessibility

MRS <Xt>, IMP\_CLUSTERCDBGDR0\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERCDBGDR0_EL1;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERCDBGDR0_EL1;

```

### A.2.2.67 IMP\_CPUPSELR\_EL1, Instruction Patch Selection Register

Selects the current instruction patch register <n> for subsequent accesses to AArch64-IMP\_CPUPCR<n>\_EL1, AArch64-IMP\_CPUPOR<n>\_EL1, and AArch64-IMP\_CPUPMR<n>\_EL1.

It is used in conjunction with AArch64-IMP\_CPUPCR\_EL1, AArch64-IMP\_CPUPOR\_EL1, and AArch64-IMP\_CPUPMR\_EL1 respectively, to access the selected register.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Generic System Control

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-127: AARCH64\_IMP\_CPUPSELR\_EL1 bit assignments

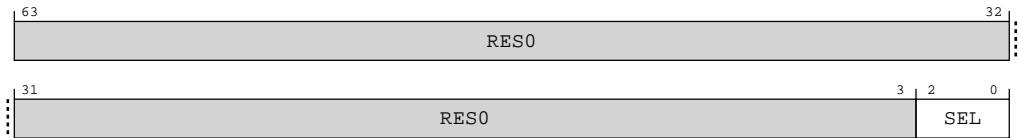


Table A-318: IMP\_CPUPSELR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0
[2:0]	SEL	Selects the current instruction patch register <n>.  If the value is greater than or equal to the number of accessible patch registers, subsequent reads and writes of AArch64-IMP_CPUPCR_EL1, AArch64-IMP_CPUPOR_EL1, and AArch64-IMP_CPUPMR_EL1 behave as <b>RAZ/WI</b> .	xxx

Access

MRS <Xt>, IMP\_CPUPSELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b000

MSR IMP\_CPUPSELR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b000

Accessibility

MRS <Xt>, IMP\_CPUPSELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPSELR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPSELR_EL1;
```

MSR IMP\_CPUPSELR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPSELR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
```

```
IMP_CPUPSELR_EL1 = X[t, 64];
```

A.2.2.68 IMP\_CPUPCR\_EL1, Selected Instruction Patch Control Register

This register accesses one of the AArch64-IMP\_CPUPCR<n>\_EL1 registers, selected by AArch64-IMP\_CPUPSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

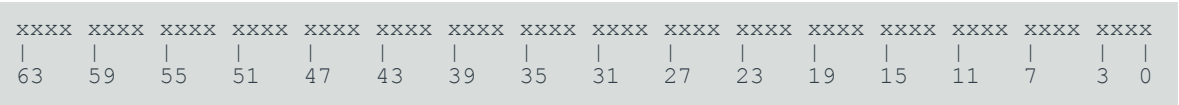
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-128: AARCH64\_IMP\_CPUPCR\_EL1 bit assignments

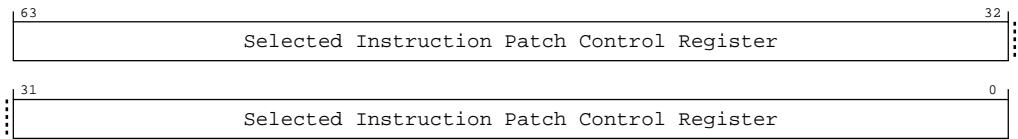


Table A-321: IMP\_CPUPCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	This register accesses AArch64-IMP_CPUPCR<n>_EL1 where n is the value in AArch64-IMP_CPUPSELR_EL1.SEL.	64 {x}

Access

If AArch64-IMP\_CPUPSELR\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPCR\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b001

MSR IMP\_CPUPCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b001

Accessibility

If AArch64-IMP\_CPUPSELR\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPCR\_EL1 behave as RAZ/WI.

MRS <Xt>, IMP\_CPUPCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPCR_EL1;
```

MSR IMP\_CPUPCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPCR_EL1 = X[t, 64];
```

A.2.2.69 IMP\_CPUPCR<n>\_EL1, Instruction Patch Control Registers, n = 0 - 5

Configures Instruction Patch n, where n is 0 to 5. This register provides **IMPLEMENTATION DEFINED** configuration and control options for the core.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-129: AARCH64\_IMP\_CPUPCR<n>\_EL1 bit assignments

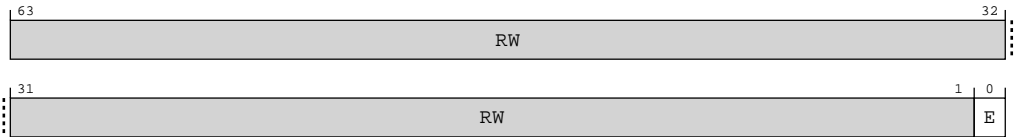


Table A-324: IMP\_CPUPCR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RW	Reserved	RW
[0]	E	Enable.  <b>0b0</b>  Any core control options affected by IMP_CPUPCR<n>_EL1, AArch64-IMP_CPUPMR<n>_EL1 and AArch64-IMP_CPUPOR<n>_EL1 are disabled.  <b>0b1</b>  <b>IMPLEMENTATION DEFINED</b> core control options enabled. Arm strongly recommends that you do not set this field to 0b1 unless directed by Arm.	0b0

Access

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPCR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPCR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPCR<n>\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b001

MSR IMP\_CPUPCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b001

Accessibility

Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPCR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPCR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPCR<n>\_EL1 behave as RAZ/WI.

MRS <Xt>, IMP\_CPUPCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPCR_EL1;
```

MSR IMP\_CPUPCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPCR_EL1 = X[t, 64];
```



A.2.2.70 IMP\_CPUPOR\_EL1, Selected Instruction Patch Opcode Register

This register accesses one of the AArch64-IMP\_CPUPOR<n>\_EL1 registers, selected by AArch64-IMP\_CPUPSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

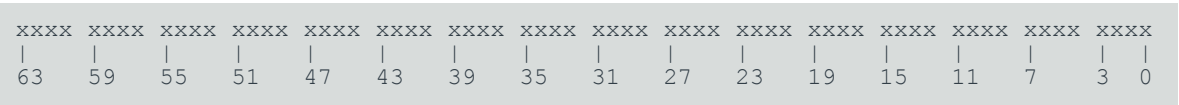
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-130: AARCH64\_IMP\_CPUPOR\_EL1 bit assignments

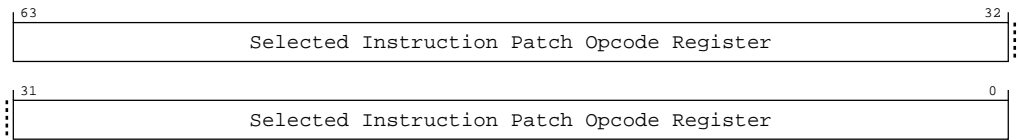


Table A-327: IMP\_CPUPOR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	This register accesses AArch64-IMP_CPUPOR<n>_EL1 where n is the value in AArch64-IMP_CPUPSELR_EL1.SEL.	64 { x }

Access

If AArch64-IMP\_CPUPSELR\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPOR\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPOR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b010

MSR IMP\_CPUPOR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b010

Accessibility

If AArch64-IMP\_CPUPSEL\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPOR\_EL1 behave as RAZ/WI.  
MRS <Xt>, IMP\_CPUPOR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPOR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPOR_EL1;
```

MSR IMP\_CPUPOR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPOR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPOR_EL1 = X[t, 64];
```

A.2.2.71 IMP\_CPUPOR<n>\_EL1, Instruction Patch Opcode Registers, n = 0 - 5

Opcode for Instruction Patch n, where n is 0 to 5. This register provides **IMPLEMENTATION DEFINED** configuration and control options for the core. This register has no effect when AArch64-IMP\_CPUPOR<n>\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

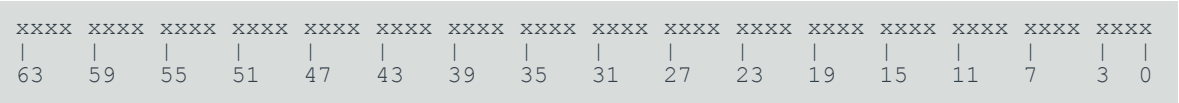
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-131: AARCH64\_IMP\_CPUPOR<n>\_EL1 bit assignments

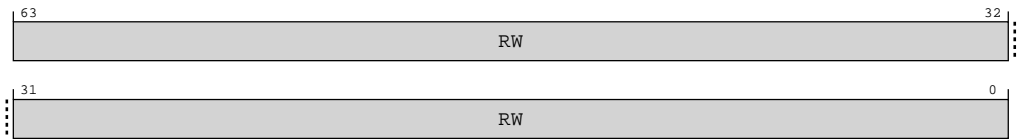


Table A-330: IMP\_CPUPOR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RW	Reserved	RW

Access

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPOR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPOR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPOR<n>\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPOR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b010

MSR IMP\_CPUPOR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b010

## Accessibility

Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPOR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPOR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPOR<n>\_EL1 behave as RAZ/WI.

MRS <Xt>, IMP\_CPUPOR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CPUPOR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPOR_EL1;

```

MSR IMP\_CPUPOR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPOR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPOR_EL1 = X[t, 64];

```

### A.2.2.72 IMP\_CPUPMR\_EL1, Selected Instruction Patch Mask Register

This register accesses one of the AArch64-IMP\_CPUPMR<n>\_EL1 registers, selected by AArch64-IMP\_CPUPSELR\_EL1.SEL.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

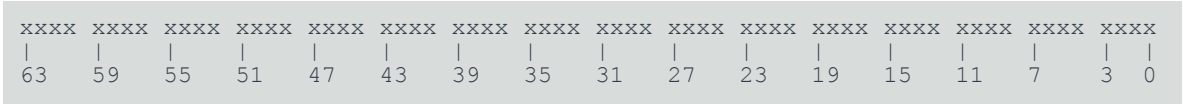
### Functional group

Generic System Control

### Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-132: AArch64\_IMP\_CPUPMR\_EL1 bit assignments

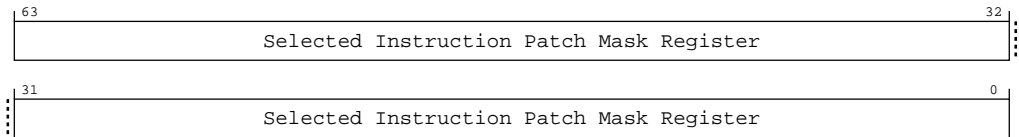


Table A-333: IMP\_CPUPMR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	This register accesses AArch64-IMP_CPUPMR<n>_EL1 where n is the value in AArch64-IMP_CPUPSELR_EL1.SEL.	64 {x}

Access

If AArch64-IMP\_CPUPSELR\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPMR\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPMR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b011

MSR IMP\_CPUPMR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b011

Accessibility

If AArch64-IMP\_CPUPSELR\_EL1 is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPMR\_EL1 behave as RAZ/WI.

MRS <Xt>, IMP\_CPUPMR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = IMP_CPUPMR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPMR_EL1;
```

MSR IMP\_CPUPMR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPMR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPMR_EL1 = X[t, 64];
```

A.2.2.73 IMP\_CPUPMR<n>\_EL1, Instruction Patch Mask Registers, n = 0 - 5

Mask for Instruction Patch n, where n is 0 to 5. This register provides **IMPLEMENTATION DEFINED** configuration and control options for the core. This register has no effect when AArch64-IMP\_CPUPCR<n>\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-133: AARCH64\_IMP\_CPUPMR<n>\_EL1 bit assignments

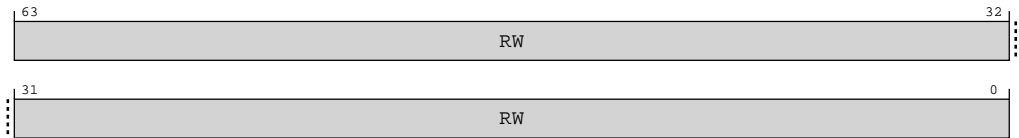


Table A-336: IMP\_CPUPMR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RW	Reserved	RW

Access

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPMR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPMR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPMR<n>\_EL1 behave as **RAZ/WI**.

MRS <Xt>, IMP\_CPUPMR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b011

MSR IMP\_CPUPMR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b010	0b1111	0b1000	0b011

Accessibility

Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

IMP\_CPUPMR<n>\_EL1 can only be accessed by using AArch64-IMP\_CPUPMR\_EL1 with AArch64-IMP\_CPUPSELR\_EL1.SEL set to n.

If <n> is greater than or equal to the number of accessible patch registers, reads and writes of IMP\_CPUPMR<n>\_EL1 behave as RAZ/WI.

MRS <Xt>, IMP\_CPUPMR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = IMP_CPUPMR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CPUPMR_EL1;
```

MSR IMP\_CPUPMR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.PATCH == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CPUPMR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CPUPMR_EL1 = X[t, 64];
```

A.2.2.74 NZCV, Condition Flags

Allows access to the condition flags.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-134: AARCH64\_NZCV bit assignments

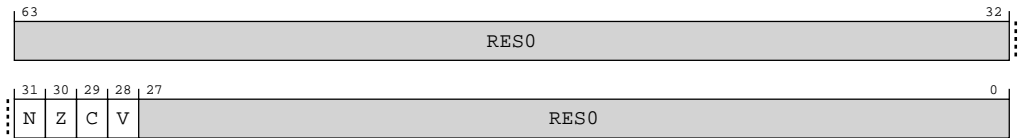


Table A-339: NZCV bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	N	Negative condition flag. Set to 1 if the result of the last flag-setting instruction was negative.	x
[30]	Z	Zero condition flag. Set to 1 if the result of the last flag-setting instruction was zero, and to 0 otherwise. A result of zero often indicates an equal result from a comparison.	x
[29]	C	Carry condition flag. Set to 1 if the last flag-setting instruction resulted in a carry condition, for example an unsigned overflow on an addition.	x
[28]	V	Overflow condition flag. Set to 1 if the last flag-setting instruction resulted in an overflow condition, for example a signed overflow on an addition.	x
[27:0]	RES0	Reserved	RES0

Access

MRS <Xt>, NZCV

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b000

MSR NZCV, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b000

Accessibility

MRS <Xt>, NZCV

```
if PSTATE.EL == EL0 then
    X[t, 64] = Zeros(32):PSTATE.<N,Z,C,V>:Zeros(28);
elseif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(32):PSTATE.<N,Z,C,V>:Zeros(28);
elseif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(32):PSTATE.<N,Z,C,V>:Zeros(28);
```

MSR NZCV, <Xt>

```
if PSTATE.EL == EL0 then
    PSTATE.<N,Z,C,V> = X[t, 64]<31:28>;
elseif PSTATE.EL == EL1 then
    PSTATE.<N,Z,C,V> = X[t, 64]<31:28>;
```

```
elseif PSTATE.EL == EL2 then
    PSTATE.<N,Z,C,V> = X[t, 64]<31:28>;
```

A.2.2.75 DAIF, Interrupt Mask Bits

Allows access to the interrupt mask bits.

Configurations

This register is available in all configurations.

Attributes

Width

64

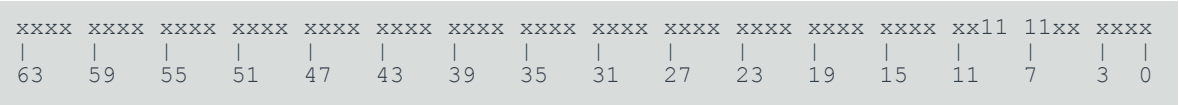
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-135: AARCH64\_DAIF bit assignments

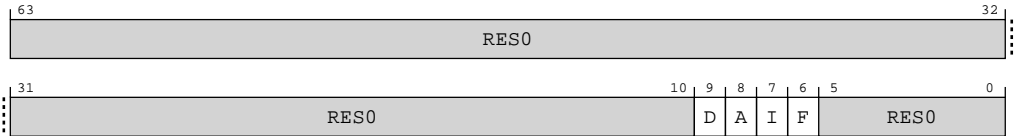


Table A-342: DAIF bit descriptions

Bits	Name	Description	Reset
[63:10]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[9]	D	Process state D mask.  <b>0b0</b> Watchpoint, Breakpoint, and Software Step exceptions targeted at the current Exception level are not masked.  <b>0b1</b> Watchpoint, Breakpoint, and Software Step exceptions targeted at the current Exception level are masked.  When the target Exception level of the debug exception is higher than the current Exception level, the exception is not masked by this bit.	0b1
[8]	A	SError interrupt mask bit.  <b>0b0</b> Exception not masked.  <b>0b1</b> Exception masked.	0b1
[7]	I	IRQ mask bit.  <b>0b0</b> Exception not masked.  <b>0b1</b> Exception masked.	0b1
[6]	F	FIQ mask bit.  <b>0b0</b> Exception not masked.  <b>0b1</b> Exception masked.	0b1
[5:0]	RES0	Reserved	RES0

## Access

MRS <Xt>, DAIF

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b001

MSR DAIF, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b001

MSR DAIFSet, #<imm>

op0	op1	CRn	op2
0b00	0b011	0b0100	0b110

MSR DAIFClr, #<imm>

op0	op1	CRn	op2
0b00	0b011	0b0100	0b111

## Accessibility

MRS <Xt>, DAIF

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.UMA == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            X[t, 64] = Zeros(54):PSTATE.<D,A,I,F>:Zeros(6);
    elseif PSTATE.EL == EL1 then
        X[t, 64] = Zeros(54):PSTATE.<D,A,I,F>:Zeros(6);
    elseif PSTATE.EL == EL2 then
        X[t, 64] = Zeros(54):PSTATE.<D,A,I,F>:Zeros(6);

```

MSR DAIF, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.UMA == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            PSTATE.<D,A,I,F> = X[t, 64]<9:6>;
    elseif PSTATE.EL == EL1 then
        PSTATE.<D,A,I,F> = X[t, 64]<9:6>;
    elseif PSTATE.EL == EL2 then
        PSTATE.<D,A,I,F> = X[t, 64]<9:6>;

```

MSR DAIFSet, #<imm>

MSR DAIFClr, #<imm>

## A.2.2.76 DIT, Data Independent Timing

Allows access to the Data Independent Timing bit.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-136: AARCH64\_DIT bit assignments

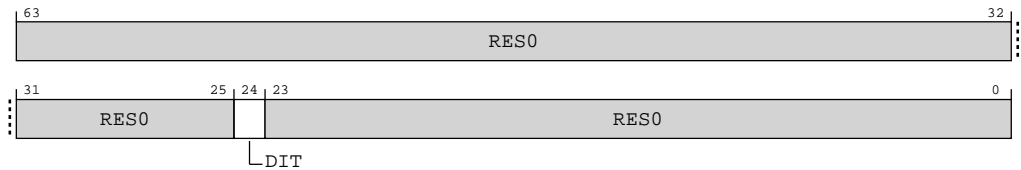


Table A-347: DIT bit descriptions

Bits	Name	Description	Reset
[63:25]	RES0	Reserved	RES0



op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b101

MSR DIT, #<imm>

op0	op1	CRn	op2
0b00	0b011	0b0100	0b010

Accessibility

MRS <Xt>, DIT

```
if PSTATE.EL == EL0 then
    X[t, 64] = Zeros(39):PSTATE.DIT:Zeros(24);
elseif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(39):PSTATE.DIT:Zeros(24);
elseif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(39):PSTATE.DIT:Zeros(24);
```

MSR DIT, <Xt>

```
if PSTATE.EL == EL0 then
    PSTATE.DIT = X[t, 64]<24>;
elseif PSTATE.EL == EL1 then
    PSTATE.DIT = X[t, 64]<24>;
elseif PSTATE.EL == EL2 then
    PSTATE.DIT = X[t, 64]<24>;
```

MSR DIT, #<imm>

A.2.2.77 SSBS, Speculative Store Bypass Safe

Allows access to the Speculative Store Bypass Safe bit.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

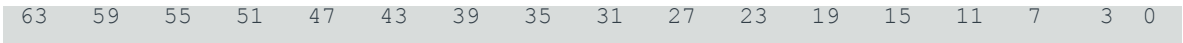
Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-137: AARCH64\_SSBS bit assignments

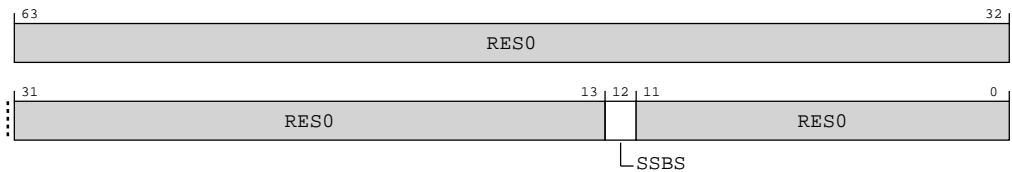


Table A-351: SSBS bit descriptions

Bits	Name	Description	Reset
[63:13]	RES0	Reserved	RES0
[12]	SSBS	<p>Speculative Store Bypass Safe.</p> <p>Prohibits speculative loads or stores which might practically allow a cache timing side channel.</p> <p>A cache timing side channel might be exploited where a load or store uses an address that is derived from a register that is being loaded from memory using a load instruction speculatively read from a memory location. If PSTATE.SSBS is enabled, the address derived from the load instruction might be from earlier in the coherence order than the latest store to that memory location with the same virtual address.</p> <p><b>0b0</b></p> <p>Hardware is not permitted to load or store speculatively, in a manner that could practically give rise to a cache timing side channel, using an address derived from a register value that has been loaded from memory using a load instruction (L) that speculatively reads an entry from earlier in the coherence order from that location being loaded from than the entry generated by the latest store (S) to that location using the same virtual address as L.</p> <p><b>0b1</b></p> <p>Hardware is permitted to load or store speculatively, in a manner that could practically give rise to a cache timing side channel, using an address derived from a register value that has been loaded from memory using a load instruction (L) that speculatively reads an entry from earlier in the coherence order fro that location being loaded from than the entry generated by the latest store (S) to that location using the same virtual address as L.</p> <p>The value of this bit is set to the value in the SCTLR_ELx.DSSBS field on taking an exception to ELx.</p>	x
[11:0]	RES0	Reserved	RES0

Access

MRS <Xt>, SSBS



op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b110

MSR SSBS, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0010	0b110

MSR SSBS, #<imm>

op0	op1	CRn	op2
0b00	0b011	0b0100	0b001

Accessibility

MRS <Xt>, SSBS

```
if PSTATE.EL == EL0 then
    X[t, 64] = Zeros(51):PSTATE.SSBS:Zeros(12);
elsif PSTATE.EL == EL1 then
    X[t, 64] = Zeros(51):PSTATE.SSBS:Zeros(12);
elsif PSTATE.EL == EL2 then
    X[t, 64] = Zeros(51):PSTATE.SSBS:Zeros(12);
```

MSR SSBS, <Xt>

```
if PSTATE.EL == EL0 then
    PSTATE.SSBS = X[t, 64]<12>;
elsif PSTATE.EL == EL1 then
    PSTATE.SSBS = X[t, 64]<12>;
elsif PSTATE.EL == EL2 then
    PSTATE.SSBS = X[t, 64]<12>;
```

MSR SSBS, #<imm>

A.2.2.78 FPCR, Floating-point Control Register

Controls floating-point behavior.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

RAZWI

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	x000	0xx0	0000	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-138: AARCH64\_FPCR bit assignments

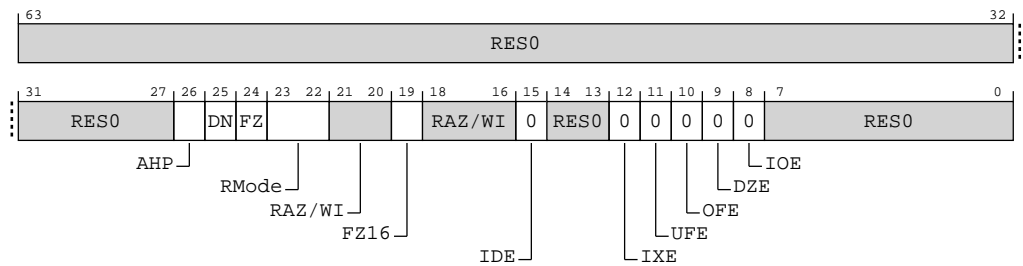


Table A-355: FPCR bit descriptions

Bits	Name	Description	Reset
[63:27]	RES0	Reserved	RES0
[26]	AHP	Alternative half-precision control bit.  <b>0b0</b> IEEE half-precision format selected.  <b>0b1</b> Alternative half-precision format selected.  This bit is used only for conversions between half-precision floating-point and other floating-point formats.  The data-processing instructions added as part of the FEAT_FP16 extension always use the IEEE half-precision format, and ignore the value of this bit.	x

Bits	Name	Description	Reset
[25]	DN	<p>Default NaN use for NaN propagation.</p> <p><b>0b0</b> NaN operands propagate through to the output of a floating-point operation.</p> <p><b>0b1</b> Any operation involving one or more NaNs returns the Default NaN.</p> <p>This bit has no effect on the output of FABS, FMAX*, FMIN*, and FNEG instructions, and a default NaN is never returned as a result of these instructions.</p> <p>The value of this bit controls both scalar and Advanced SIMD floating-point arithmetic.</p>	x
[24]	FZ	<p>Flushing denormalized numbers to zero control bit.</p> <p><b>0b0</b> Flushing denormalized numbers to zero disabled.</p> <p><b>0b1</b> Flushing denormalized numbers to zero enabled.</p> <p>For more information, see <i>Flushing denormalized numbers to zero</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> and the pseudocode of the floating-point instructions.</p>	x
[23:22]	RMode	<p>Rounding Mode control field.</p> <p><b>0b00</b> Round to Nearest (RN) mode.</p> <p><b>0b01</b> Round towards Plus Infinity (RP) mode.</p> <p><b>0b10</b> Round towards Minus Infinity (RM) mode.</p> <p><b>0b11</b> Round towards Zero (RZ) mode.</p> <p>The specified rounding mode is used by both scalar and Advanced SIMD floating-point instructions.</p>	xx
[21:20]	RAZ/WI	Reserved	RAZ/ WI
[19]	FZ16	<p><b>When IsFeatureImplemented(FEAT_FP16)</b> Flushing denormalized numbers to zero control bit on half-precision data-processing instructions.</p> <p><b>0b0</b> For some instructions, this bit disables flushing to zero of inputs and outputs that are half-precision denormalized numbers.</p> <p><b>0b1</b> Flushing denormalized numbers to zero enabled.</p> <p>The value of this bit applies to both scalar and Advanced SIMD floating-point half-precision calculations.</p> <p>For more information, see <i>Flushing denormalized numbers to zero</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> and the pseudocode of the floating-point instructions.</p> <p><b>Otherwise</b> RES0</p>	xxxx

Bits	Name	Description	Reset
[18:16]	<b>RAZ/WI</b>	Reserved	<b>RAZ/WI</b>
[15]	IDE	Input Denormal floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.IDC bit is set to 1.	0b0
[14:13]	<b>RES0</b>	Reserved	<b>RES0</b>
[12]	IXE	Inexact floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.IXC bit is set to 1.	0b0
[11]	UFE	Underflow floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.UFC bit is set to 1.	0b0
[10]	OFE	Overflow floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.OFC bit is set to 1.	0b0
[9]	DZE	Divide by Zero floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.DZC bit is set to 1.	0b0
[8]	IOE	Invalid Operation floating-point exception trap enable.  <b>0b0</b> Untrapped exception handling selected. If the floating-point exception occurs, the AArch64-FPSR.IOC bit is set to 1.	0b0
[7:0]	<b>RES0</b>	Reserved	<b>RES0</b>

## Access

MRS <Xt>, FPCR

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0100	0b000

MSR FPCR, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0100	0b000

## Accessibility

MRS <Xt>, FPCR

```
if PSTATE.EL == EL0 then
    if CPACR_EL1.FPEN != '11' then
```

```

        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x00);
        else
            AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            X[t, 64] = FPCR;
    elsif PSTATE.EL == EL1 then
        if CPACR_EL1.FPEN == 'x0' then
            AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            X[t, 64] = FPCR;
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            X[t, 64] = FPCR;

```

#### MSR FPCR, <Xt>

```

    if PSTATE.EL == EL0 then
        if CPACR_EL1.FPEN != '11' then
            if HCR_EL2.TGE == '1' then
                AArch64.SystemAccessTrap(EL2, 0x00);
            else
                AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            FPCR = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if CPACR_EL1.FPEN == 'x0' then
            AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            FPCR = X[t, 64];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            FPCR = X[t, 64];

```

### A.2.2.79 FPSR, Floating-point Status Register

Provides floating-point system status information.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic System Control

**Access type**

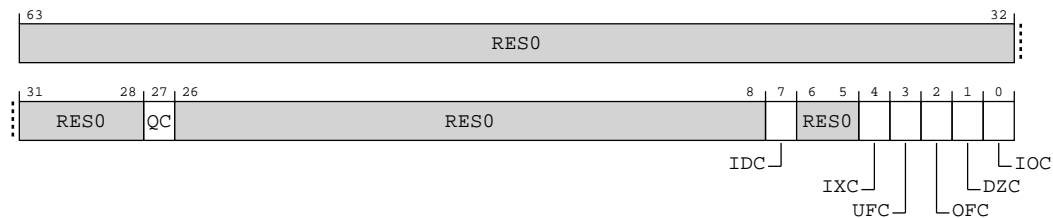
See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

**Note**

Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure A-139: AARCH64\_FPSR bit assignments****Table A-358: FPSR bit descriptions**

Bits	Name	Description	Reset
[63:28]	RES0	Reserved	RES0
[27]	QC	Cumulative saturation bit, Advanced SIMD only. This bit is set to 1 to indicate that an Advanced SIMD integer operation has saturated since 0 was last written to this bit.	x
[26:8]	RES0	Reserved	RES0
[7]	IDC	Input Denormal cumulative floating-point exception bit. This bit is set to 1 to indicate that the Input Denormal floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.IDE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.IDE is 0.	x
[6:5]	RES0	Reserved	RES0
[4]	IXC	Inexact cumulative floating-point exception bit. This bit is set to 1 to indicate that the Inexact floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.IXE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.IXE is 0.  The criteria for the Inexact floating-point exception to occur are affected by whether denormalized numbers are flushed to zero and by the value of the AArch64-FPCR.AH bit. For more information, see <i>Floating-point exceptions and exception traps</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x

Bits	Name	Description	Reset
[3]	UFC	Underflow cumulative floating-point exception bit. This bit is set to 1 to indicate that the Underflow floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.UFE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.UFE is 0 or if flushing denormalized numbers to zero is enabled.  The criteria for the Underflow floating-point exception to occur are affected by whether denormalized numbers are flushed to zero and by the value of the AArch64-FPCR.AH bit. For more information, see <i>Floating-point exceptions and exception traps</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x
[2]	OFC	Overflow cumulative floating-point exception bit. This bit is set to 1 to indicate that the Overflow floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.OFE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.OFE is 0.	x
[1]	DZC	Divide by Zero cumulative floating-point exception bit. This bit is set to 1 to indicate that the Divide by Zero floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.DZE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.DZE is 0.	x
[0]	IOC	Invalid Operation cumulative floating-point exception bit. This bit is set to 1 to indicate that the Invalid Operation floating-point exception has occurred since 0 was last written to this bit.  How scalar and Advanced SIMD floating-point instructions update this bit depends on the value of the AArch64-FPCR.IOE bit. This bit is set to 1 to indicate a floating-point exception only if AArch64-FPCR.IOE is 0.  The criteria for the Invalid Operation floating-point exception to occur are affected by the value of the AArch64-FPCR.AH bit. For more information, see <i>Floating-point exceptions and exception traps</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x

## Access

MRS <Xt>, FPSR

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0100	0b001

MSR FPSR, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0100	0b001

## Accessibility

MRS <Xt>, FPSR

```

if PSTATE.EL == EL0 then
    if CPACR_EL1.FPEN != '11' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x00);
        else
            AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then

```

```

        AArch64.SystemAccessTrap(EL2, 0x07);
    else
        X[t, 64] = FPSR;
    elsif PSTATE.EL == EL1 then
        if CPACR_EL1.FPEN == 'x0' then
            AArch64.SystemAccessTrap(EL1, 0x07);
        elsif CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            X[t, 64] = FPSR;
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TFP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x07);
        else
            X[t, 64] = FPSR;

```

MSR FPSR, <Xt>

```

if PSTATE.EL == EL0 then
    if CPACR_EL1.FPEN != '11' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x00);
        else
            AArch64.SystemAccessTrap(EL1, 0x07);
    elsif CPTR_EL2.TFP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x07);
    else
        FPSR = X[t, 64];
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.FPEN == 'x0' then
        AArch64.SystemAccessTrap(EL1, 0x07);
    elsif CPTR_EL2.TFP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x07);
    else
        FPSR = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TFP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x07);
    else
        FPSR = X[t, 64];

```

#### A.2.2.80 TPIDR\_ELO, ELO Read/Write Software Thread ID Register

Provides a location where software executing at EL0 can store thread identifying information, for OS management purposes.

The PE makes no use of this register.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

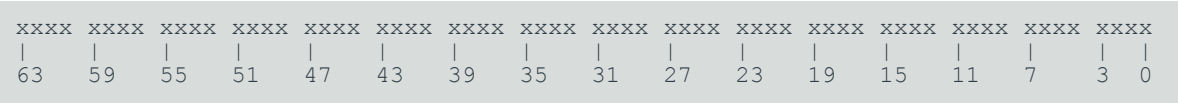
Generic System Control



Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-140: AARCH64\_TPIDR\_ELO bit assignments

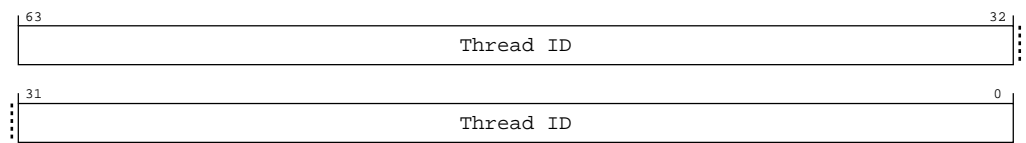


Table A-361: TPIDR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Thread ID. Thread identifying information stored by software running at this Exception level.	64 {x}

Access

MRS <Xt>, TPIDR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1101	0b0000	0b010

MSR TPIDR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1101	0b0000	0b010

Accessibility

MRS <Xt>, TPIDR\_ELO

```
if PSTATE.EL == EL0 then
    X[t, 64] = TPIDR_ELO;
elsif PSTATE.EL == EL1 then
    X[t, 64] = TPIDR_ELO;
elsif PSTATE.EL == EL2 then
    X[t, 64] = TPIDR_ELO;
```

MSR TPIDR\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    TPIDR_ELO = X[t, 64];
elsif PSTATE.EL == EL1 then
    TPIDR_ELO = X[t, 64];
elsif PSTATE.EL == EL2 then
    TPIDR_ELO = X[t, 64];
```

A.2.2.81 TPIDRRO\_ELO, ELO Read-Only Software Thread ID Register

Provides a location where software executing at EL1 or higher can store thread identifying information that is visible to software executing at EL0, for OS management purposes.

The PE makes no use of this register.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-141: AARCH64\_TPIDRRO\_ELO bit assignments

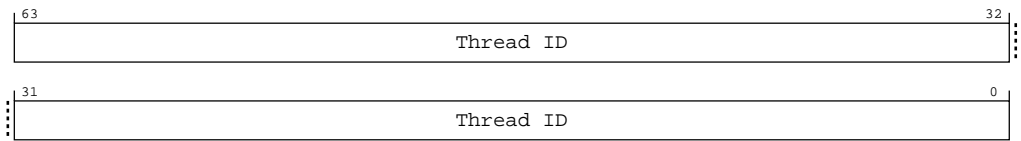


Table A-364: TPIDRRO\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Thread ID. Thread identifying information stored by software running at this Exception level.	64 {x}

Access

MRS <Xt>, TPIDRRO\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b11101	0b0000	0b011

MSR TPIDRRO\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b11101	0b0000	0b011

Accessibility

MRS <Xt>, TPIDRRO\_ELO

```
if PSTATE.EL == EL0 then
    X[t, 64] = TPIDRRO_ELO;
elsif PSTATE.EL == EL1 then
    X[t, 64] = TPIDRRO_ELO;
elsif PSTATE.EL == EL2 then
    X[t, 64] = TPIDRRO_ELO;
```

MSR TPIDRRO\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    TPIDRRO_ELO = X[t, 64];
elsif PSTATE.EL == EL2 then
    TPIDRRO_ELO = X[t, 64];
```

A.2.2.82 MPUIR\_EL2, MPU Type Register (EL2)

Identifies the number of regions supported by the EL2 MPU.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-142: AARCH64\_MPUIR\_EL2 bit assignments

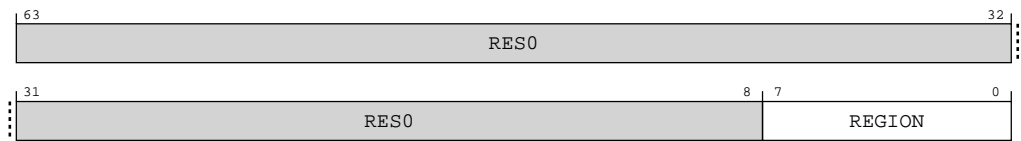


Table A-367: MPUIR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	REGION	The number of EL2 MPU regions supported.	8 {x}

Access

MRS <Xt>, MPUIR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0000	0b0000	0b100

Accessibility

MRS <Xt>, MPUIR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MPUIR_EL2;
```

A.2.2.83 ACTLR\_EL2, Auxiliary Control Register (EL2)

Provides **IMPLEMENTATION DEFINED** configuration and control options for EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-143: AARCH64\_ACTLR\_EL2 bit assignments

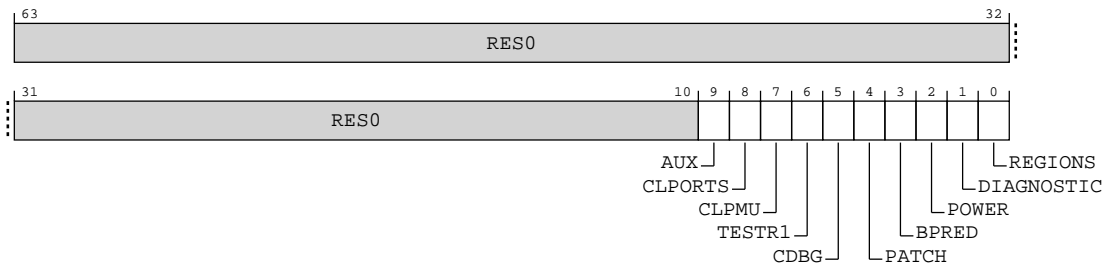


Table A-369: ACTLR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:10]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[9]	AUX	<p>Auxiliary registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUACTLR_EL1 and AArch64-IMP_CLUSTERACTLR_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUACTLR_EL1 and AArch64-IMP_CLUSTERACTLR_EL1 are allowed.</p>	0b0
[8]	CLPORTS	<p>Cluster L2 partitioning and ports registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_CLUSTERQOSR_EL1, AArch64-IMP_CLUSTERACELCTLR_EL1, AArch64-IMP_CLUSTERSID_EL1, AArch64-IMP_CLUSTERACPSID_EL1 and AArch64-IMP_CLUSTERPARTCR_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_CLUSTERQOSR_EL1, AArch64-IMP_CLUSTERACELCTLR_EL1, AArch64-IMP_CLUSTERSID_EL1, AArch64-IMP_CLUSTERACPSID_EL1 and AArch64-IMP_CLUSTERPARTCR_EL1 are allowed.</p>	0b0
[7]	CLPMU	<p>Cluster Performance Monitor Unit registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_CLUSTERPMCR_EL1, AArch64-IMP_CLUSTERPMCNTENSET_EL1, AArch64-IMP_CLUSTERPMCNTENCLR_EL1, AArch64-IMP_CLUSTERPMOVSET_EL1, AArch64-IMP_CLUSTERPMOVCLR_EL1, AArch64-IMP_CLUSTERPMSELR_EL1, AArch64-IMP_CLUSTERPMINTENSET_EL1, AArch64-IMP_CLUSTERPMINTENCLR_EL1, AArch64-IMP_CLUSTERPMCCNTR_EL1, AArch64-IMP_CLUSTERPMXEVTYPYR_EL1, AArch64-IMP_CLUSTERPMXVCNTR_EL1, AArch64-IMP_CLUSTERPMCLAIMCLR_EL1 and AArch64-IMP_CLUSTERPMCLAIMSET_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_CLUSTERPMCR_EL1, AArch64-IMP_CLUSTERPMCNTENSET_EL1, AArch64-IMP_CLUSTERPMCNTENCLR_EL1, AArch64-IMP_CLUSTERPMOVSET_EL1, AArch64-IMP_CLUSTERPMOVCLR_EL1, AArch64-IMP_CLUSTERPMSELR_EL1, AArch64-IMP_CLUSTERPMINTENSET_EL1, AArch64-IMP_CLUSTERPMINTENCLR_EL1, AArch64-IMP_CLUSTERPMCCNTR_EL1, AArch64-IMP_CLUSTERPMXEVTYPYR_EL1, AArch64-IMP_CLUSTERPMXVCNTR_EL1, AArch64-IMP_CLUSTERPMCLAIMCLR_EL1 and AArch64-IMP_CLUSTERPMCLAIMSET_EL1 are allowed.</p>	0b0
[6]	TESTR1	<p>Testing registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_TESTR1_EL1, AArch64-IMP_TESTR2_EL1 and AArch64-IMP_TESTR1KEY_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_TESTR1_EL1, AArch64-IMP_TESTR2_EL1 and AArch64-IMP_TESTR1KEY_EL1 are allowed.</p>	0b0

Bits	Name	Description	Reset
[5]	CDBG	<p>Cache debug registers read/write control.</p> <p><b>0b0</b></p> <p>Read accesses from EL1 to AArch64-IMP_CDBGDR0_EL1, AArch64-IMP_CDBGDR1_EL1 and AArch64-IMP_CLUSTERCDBGDR0_EL1, as well as executing from EL1 SYS_IMP_CDBGDCT, SYS_IMP_CDBGICT, SYS_IMP_CDBGTT, SYS_IMP_CDBGDCD, SYS_IMP_CDBGICD, SYS_IMP_CDBGTD, SYS_IMP_CLUSTERCDBGL2D, SYS_IMP_CLUSTERCDBGL2DT, SYS_IMP_CLUSTERCDBGL2T, SYS_IMP_CLUSTERCDBGLCUDT are trapped to EL2.</p> <p><b>0b1</b></p> <p>Read accesses from EL1 to AArch64-IMP_CDBGDR0_EL1, AArch64-IMP_CDBGDR1_EL1 and AArch64-IMP_CLUSTERCDBGDR0_EL1, as well as executing from EL1 SYS_IMP_CDBGDCT, SYS_IMP_CDBGICT, SYS_IMP_CDBGTT, SYS_IMP_CDBGDCD, SYS_IMP_CDBGICD, SYS_IMP_CDBGTD, SYS_IMP_CLUSTERCDBGL2D, SYS_IMP_CLUSTERCDBGL2DT, SYS_IMP_CLUSTERCDBGL2T, SYS_IMP_CLUSTERCDBGLCUDT are allowed.</p>	0b0
[4]	PATCH	<p>Patch registers read/write control.</p> <p><b>0b0</b></p> <p>Read and write accesses from EL1 to AArch64-IMP_CPUPSELR_EL1, AArch64-IMP_CPUPCR_EL1, AArch64-IMP_CPUPOR_EL1 and AArch64-IMP_CPUPMR_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Read and write accesses from EL1 to AArch64-IMP_CPUPSELR_EL1, AArch64-IMP_CPUPCR_EL1, AArch64-IMP_CPUPOR_EL1 and AArch64-IMP_CPUPMR_EL1 are allowed.</p>	0b0
[3]	BPRED	<p>Branch prediction registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_BPCTLR_EL1 as well as executing from EL1 SYS-IMP_BPI are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_BPCTLR_EL1 as well as executing from EL1 SYS-IMP_BPI are allowed.</p>	0b0
[2]	POWER	<p>Power registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUPWRCTLR_EL1, AArch64-IMP_CLUSTERPWRCTLR_EL1 and AArch64-IMP_CLUSTERPWRDN_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUPWRCTLR_EL1, AArch64-IMP_CLUSTERPWRCTLR_EL1 and AArch64-IMP_CLUSTERPWRDN_EL1 are allowed.</p>	0b0
[1]	DIAGNOSTIC	<p>Diagnostic registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUBUSTIMEOUTR_EL1, AArch64-IMP_CLUSTERBUSTIMEOUTR_EL1, AArch64-IMP_INTMONR_EL1, AArch64-IMP_MEMPROTCTLR_EL1 and AArch64-IMP_CLUSTERMEMPROTCTLR_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_CPUBUSTIMEOUTR_EL1, AArch64-IMP_CLUSTERBUSTIMEOUTR_EL1, AArch64-IMP_INTMONR_EL1, AArch64-IMP_MEMPROTCTLR_EL1 and AArch64-IMP_CLUSTERMEMPROTCTLR_EL1 are allowed.</p>	0b0

Bits	Name	Description	Reset
[0]	REGIONS	<p>Region registers write control.</p> <p><b>0b0</b></p> <p>Write accesses from EL1 to AArch64-IMP_ITCMREGIONR_EL1, AArch64-IMP_DTCMREGIONR_EL1, AArch64-IMP_LLPPREGIONR_EL1, AArch64-IMP_SPPREGIONR_EL1 and AArch64-IMP_LLDRAMREGIONR_EL1 are trapped to EL2.</p> <p><b>0b1</b></p> <p>Write accesses from EL1 to AArch64-IMP_ITCMREGIONR_EL1, AArch64-IMP_DTCMREGIONR_EL1, AArch64-IMP_LLPPREGIONR_EL1, AArch64-IMP_SPPREGIONR_EL1 and AArch64-IMP_LLDRAMREGIONR_EL1 are allowed.</p>	0b0

### Access

MRS <Xt>, ACTLR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0000	0b001

MSR ACTLR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0000	0b001

### Accessibility

MRS <Xt>, ACTLR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ACTLR_EL2;

```

MSR ACTLR\_EL2, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    ACTLR_EL2 = X[t, 64];

```

## A.2.2.84 HCR\_EL2, Hypervisor Configuration Register

Provides configuration controls for virtualization, including defining whether various operations are trapped to EL2.

### Configurations

This register is available in all configurations.



Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x0xx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-144: AARCH64\_HCR\_EL2 bit assignments

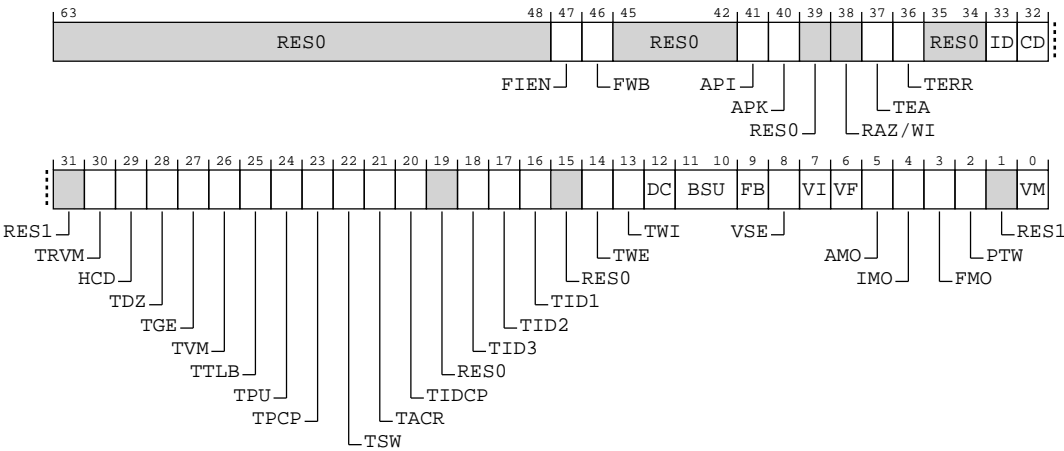


Table A-372: HCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47]	FIEN	<p>Fault Injection Enable. Unless this bit is set to 1, accesses to the AArch64-ERXPFPGCDN_EL1, AArch64-ERXPFPGCTL_EL1, and AArch64-ERXPFPGF_EL1 registers from EL1 generate a Trap exception to EL2, when EL2 is enabled in the current Security state, reported using EC syndrome value 0x18.</p> <p><b>0b0</b></p> <p>Accesses to the specified registers from EL1 are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[46]	FWB	<p>Forced Write-Back. Defines the combined cacheability attributes in a 2 stage translation regime.</p> <p><b>0b0</b></p> <p>When this bit is 0, then:</p> <ul style="list-style-type: none"> <li>The combination of stage 1 and stage 2 translations on memory type and cacheability attributes are as described in the Armv8.0 architecture. For more information, see <i>Combining stage 1 and stage 2 memory type attributes</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</li> <li>The encoding of the stage 2 memory type and cacheability attributes is derived from AArch64-MAIR_EL2 register, as described in the Armv8-R AArch64 architecture.</li> </ul> <p><b>0b1</b></p> <p>When this bit is 1, then:</p> <ul style="list-style-type: none"> <li>The inner and outer memory attributes for stage 2 EL1&amp;O translation regime must be the same with the same encoding, otherwise, the combined attribute is <b>UNKNOWN</b>.</li> <li>If stage 2 EL1&amp;O translation regime memory attribute is Write-Back with AArch64-MAIR_EL2.Attr[7:6] = 0b11, then the combined attribute is Normal Write-Back. For all other encodings, the combination of stage 1 and stage 2 translations on memory type and cacheability attributes are as described in the Armv8.0 architecture.</li> </ul> <p>This bit is permitted to be cached in a TLB.</p>	x
[45:42]	RES0	Reserved	RES0
[41]	API	<p>Controls the use of instructions related to Pointer Authentication:</p> <ul style="list-style-type: none"> <li>In EL0, the associated AArch64-SCTLR_EL1.En&lt;N&gt;&lt;M&gt;==1.</li> <li>In EL1, the associated AArch64-SCTLR_EL1.En&lt;N&gt;&lt;M&gt;==1.</li> </ul> <p>Traps are reported using EC syndrome value 0x09. The Pointer Authentication instructions trapped are:</p> <ul style="list-style-type: none"> <li>AUTDA, AUTDB, AUTDZA, AUTDZB, AUTIA, AUTIA1716, AUTIASP, AUTIAZ, AUTIB, AUTIB1716, AUTIBSP, AUTIBZ, AUTIZA, AUTIZB.</li> <li>PACGA, PACDA, PACDB, PACDZA, PACDZB, PACIA, PACIA1716, PACIASP, PACIAZ, PACIB, PACIB1716, PACIBSP, PACIBZ, PACIZA, PACIZB.</li> <li>RETAA, RETAB, BRAA, BRAB, BLRAA, BLRAB, BRAAZ, BRABZ, BLRAAZ, BLRABZ.</li> <li>ERETAA, ERETAB, LDRAA, and LDRAB.</li> </ul> <p><b>0b0</b></p> <p>The instructions related to Pointer Authentication are trapped to EL2, when EL2 is enabled in the current Security state and the instructions are enabled for the EL1&amp;O translation regime, from:</p> <ul style="list-style-type: none"> <li>EL0.</li> <li>EL1.</li> </ul> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x

Bits	Name	Description	Reset
[40]	APK	<p>Trap registers holding "key" values for Pointer Authentication. Traps accesses to the following registers from EL1 to EL2, when EL2 is enabled in the current Security state, reported using EC syndrome value 0x18:</p> <ul style="list-style-type: none"> <li>AArch64-APIAKeyLo_EL1, AArch64-APIAKeyHi_EL1, AArch64-APIBKeyLo_EL1, AArch64-APIBKeyHi_EL1, AArch64-APDAKeyLo_EL1, AArch64-APDAKeyHi_EL1, AArch64-APDBKeyLo_EL1, AArch64-APDBKeyHi_EL1, AArch64-APGAKeyLo_EL1, and AArch64-APGAKeyHi_EL1.</li> </ul> <p><b>0b0</b></p> <p>Access to the registers holding "key" values for pointer authentication from EL1 are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[39]	RES0	Reserved	RES0
[38]	RAZ/WI	Reserved	RAZ/WI
[37]	TEA	<p>Route synchronous External abort exceptions to EL2.</p> <p><b>0b0</b></p> <p>This control does not cause exceptions to be routed from EL0 and EL1 to EL2.</p> <p><b>0b1</b></p> <p>Route synchronous External abort exceptions from EL0 and EL1 to EL2, when EL2 is enabled in the current Security state.</p>	x
[36]	TERR	<p>Trap accesses of Error Record registers. Enables a trap to EL2 on accesses of Error Record registers.</p> <p><b>0b0</b></p> <p>Accesses of the specified Error Record registers are not trapped by this mechanism.</p> <p><b>0b1</b></p> <p>Accesses of the specified Error Record registers at EL1 are trapped to EL2, unless the instruction generates a higher priority exception.</p> <p>In AArch64 state, the instructions affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS and MSR accesses to AArch64-ERRSELR_EL1, AArch64-ERXADDR_EL1, AArch64-ERXCTLR_EL1, AArch64-ERXMISCO_EL1, AArch64-ERXMISC1_EL1, and AArch64-ERXSTATUS_EL1.</li> <li>MRS accesses to AArch64-ERRIDR_EL1 and AArch64-ERXFR_EL1.</li> <li>If FEAT_RASv1p1 is implemented, MRS and MSR accesses to AArch64-ERXMISC2_EL1 and AArch64-ERXMISC3_EL1.</li> </ul> <p>Unless the instruction generates a higher priority exception, trapped instructions generate an exception to EL2.</p> <p>Trapped AArch64 instructions are reported using EC syndrome value 0x18.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field is permitted to be <b>RES0</b> if all of the following are true: <ul style="list-style-type: none"> <li>AArch64-ERRSELR_EL1 and all ERX* registers are implemented as UNDEFINED or RAZ/WI.</li> <li>AArch64-ERRIDR_EL1.NUM is zero.</li> </ul> </li> </ul>	x
[35:34]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[33]	ID	<p>Stage 2 Instruction access cacheability disable. For the EL1&amp;0 translation regime, when EL2 is enabled in the current Security state and HCR_EL2.VM==1, this control forces all stage 2 translations for instruction accesses to Normal memory to be Non-cacheable.</p> <p><b>Note:</b> The behavior is the same irrespective of whether the instruction accesses are to an MPU region or Background region.</p> <p><b>0b0</b> This control has no effect on stage 2 of the EL1&amp;0 translation regime.</p> <p><b>0b1</b> Forces all stage 2 translations for instruction accesses to Normal memory to be Non-cacheable.</p> <p>This bit has no effect on the EL2 translation regime.</p>	x
[32]	CD	<p>Stage 2 Data access cacheability disable. For the EL1&amp;0 translation regime, when EL2 is enabled in the current Security state and HCR_EL2.VM==1, this control forces all stage 2 translations for data accesses and translation table walks to Normal memory to be Non-cacheable.</p> <p><b>Note:</b> The behavior is same irrespective of whether the data accesses is to MPU region or Background region.</p> <p><b>0b0</b> This control has no effect on stage 2 of the EL1&amp;0 translation regime for data accesses and translation table walks.</p> <p><b>0b1</b> Forces all stage 2 translations for data accesses and translation table walks to Normal memory to be Non-cacheable.</p> <p>This bit has no effect on the EL2 translation regime.</p>	x
[31]	RES1	Reserved	RES1

Bits	Name	Description	Reset
[30]	TRVM	<p>Trap Reads of Virtual Memory controls. Traps reads of the virtual memory control registers to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>If EL1 is using AArch64 state, EL1 accesses to the following registers are trapped to EL2 and reported using EC syndrome value 0x18 for MRS: <ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1, AArch64-TTBRO_EL1, AArch64-TTBR1_EL1, AArch64-TCR_EL1, AArch64-ESR_EL1, AArch64-FAR_EL1, AArch64-AFSR0_EL1, AArch64-AFSR1_EL1, AArch64-MAIR_EL1, AArch64-AMAIR_EL1, AArch64-CONTEXTIDR_EL1.</li> <li>If EL1 is in PMSAv8-64 context, EL1 accesses to the following registers are also trapped to EL2 and reported using EC syndrome value 0x18 - AArch64-PRENR_EL1, AArch64-PRSELR_EL1, AArch64-PRBAR_EL1, AArch64-PRBARn_EL1, AArch64-PRLAR_EL1, AArch64-PRLARn_EL1.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Read accesses to the specified Virtual Memory control registers are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p> <p><b>Note:</b> EL2 provides a second stage of address translation, that a hypervisor can use to remap the address map defined by a Guest OS. In addition, a hypervisor can trap attempts by a Guest OS to write to the registers that control the memory system. A hypervisor might use this trap as part of its virtualization of memory management.</p>	x
[29]	HCD	<p>HVC instruction disable. Disables EL1 execution of HVC instructions, from both Execution states, when EL2 is enabled in the current Security state, reported using EC syndrome value 0x00.</p> <p><b>0b0</b></p> <p>HVC instruction execution is enabled at EL2 and EL1.</p> <p><b>0b1</b></p> <p>HVC instructions are <b>UNDEFINED</b> at EL2 and EL1. Any resulting exception is taken to the Exception level at which the HVC instruction is executed.</p> <p><b>Note:</b> HVC instructions are always <b>UNDEFINED</b> at EL0.</p>	x
[28]	TDZ	<p>Trap DC ZVA instructions. Traps EL0 and EL1 execution of DC ZVA instructions to EL2, when EL2 is enabled in the current Security state, from AArch64 state only, reported using EC syndrome value 0x18.</p> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>In AArch64 state, any attempt to execute an instruction this trap applies to at EL1, or at EL0 when the instruction is not <b>UNDEFINED</b> at EL0, is trapped to EL2 when EL2 is enabled in the current Security state.</p> <p>Reading the AArch64-DCZID_EL0 returns a value that indicates that the instructions this trap applies to are not supported.</p>	x

Bits	Name	Description	Reset
[27]	TGE	<p>Trap General Exceptions, from ELO.</p> <p><b>0b0</b></p> <p>This control has no effect on execution at ELO.</p> <p><b>0b1</b></p> <p>When EL2 is not enabled in the current Security state, this control has no effect on execution at ELO.</p> <p>When EL2 is enabled in the current Security state, in all cases:</p> <ul style="list-style-type: none"> <li>• All exceptions that would be routed to EL1 are routed to EL2.</li> <li>• If EL1 is using AArch64, the AArch64-SCTLR_EL1.M field is treated as being 0 for all purposes other than returning the result of a direct read of AArch64-SCTLR_EL1.</li> <li>• If stage 1 EL1&amp;O translation regime is in PMSAv8-64 context, the AArch64-SCTLR_EL1.BR field is treated as being 0 for all purposes other than returning the result of a direct read of AArch64-SCTLR_EL1.</li> <li>• All virtual interrupts are disabled.</li> <li>• Any <b>IMPLEMENTATION DEFINED</b> mechanisms for signaling virtual interrupts are disabled.</li> <li>• An exception return to EL1 is treated as an illegal exception return.</li> <li>• The AArch64-MDCR_EL2.{TDRA, TDOSA, TDA, TDE} fields are treated as being 1 for all purposes other than returning the result of a direct read of AArch64-MDCR_EL2.</li> </ul> <p>In addition, when EL2 is enabled in the current Security state, the Effective values of the HCR_EL2.{FMO, IMO, AMO} fields are 1.</p> <p>HCR_EL2.TGE must not be cached in a TLB.</p>	x
[26]	TVM	<p>Trap Virtual Memory controls. Traps writes to the virtual memory control registers to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>• If EL1 is using AArch64 state, the following registers are trapped to EL2 and reported using EC syndrome value 0x18 for MSR: <ul style="list-style-type: none"> <li>◦ AArch64-SCTLR_EL1, AArch64-TTBRO_EL1, AArch64-TTBR1_EL1, AArch64-TCR_EL1, AArch64-ESR_EL1, AArch64-FAR_EL1, AArch64-AFSR0_EL1, AArch64-AFSR1_EL1, AArch64-MAIR_EL1, AArch64-AMAIR_EL1, AArch64-CONTEXTIDR_EL1.</li> <li>◦ If EL1 is in PMSAv8-64 context, EL1 accesses to the following registers are also trapped to EL2 and reported using EC syndrome value 0x18 - AArch64-PRENR_EL1, AArch64-PRSELR_EL1, AArch64-PRBAR_EL1, AArch64-PRBARn_EL1, AArch64-PRLAR_EL1, AArch64-PRLARn_EL1.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Write accesses to the specified Virtual Memory control registers are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p>	x

Bits	Name	Description	Reset
[25]	TTLB	<p>Trap TLB maintenance instructions. Traps EL1 execution of TLB maintenance instructions to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>When EL1 is using AArch64 state, the following instructions are trapped to EL2 and reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>TLBI VMALLE1, TLBI VAE1, TLBI ASIDE1, TLBI VAAE1, TLBI VALE1, TLBI VAALE1.</li> <li>TLBI VMALLE1IS, TLBI VAE1IS, TLBI ASIDE1IS, TLBI VAAE1IS, TLBI VALE1IS, TLBI VAALE1IS.</li> <li>If FEAT_TLBIOS is implemented, this trap applies to TLBI VMALLE1OS, TLBI VAE1OS, TLBI ASIDE1OS, TLBI VAAE1OS, TLBI VALE1OS, TLBI VAALE1OS.</li> <li>If FEAT_TLBIRANGE is implemented, this trap applies to TLBI RVAE1, TLBI RVAAE1, TLBI RVALE1, TLBI RVALE1IS, TLBI RVAE1IS, TLBI RVAAE1IS, TLBI RVALE1IS, TLBI RVALE1IS.</li> <li>If FEAT_TLBIOS and FEAT_TLBIRANGE are implemented, this trap applies to TLBI RVAE1OS, TLBI RVAE1OS, TLBI RVALE1OS, TLBI RVALE1OS, TLBI RVALE1OS.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL1 execution of the specified TLB maintenance instructions are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p> <p><b>Note:</b> The TLB maintenance instructions are <b>UNDEFINED</b> at EL0.</p>	x
[24]	TPU	<p>Trap cache maintenance instructions that operate to the Point of Unification. Traps execution of those cache maintenance instructions to EL2, when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>If EL0 is using AArch64 state and the value of AArch64-SCTLR_EL1.UCI is not 0, the following instructions are trapped to EL2 and reported with EC syndrome value 0x18: <ul style="list-style-type: none"> <li>IC IVAU, DC CVAU. If the value of AArch64-SCTLR_EL1.UCI is 0 these instructions are <b>UNDEFINED</b> at EL0 and any resulting exception is higher priority than this trap to EL2.</li> </ul> </li> <li>If EL1 is using AArch64 state, the following instructions are trapped to EL2 and reported with EC syndrome value 0x18: <ul style="list-style-type: none"> <li>IC IVAU, IC IALLU, IC IALLUIS, DC CVAU.</li> </ul> </li> </ul> <p><b>Note:</b> An exception generated because an instruction is <b>UNDEFINED</b> at EL0 is higher priority than this trap to EL2. In addition:</p> <ul style="list-style-type: none"> <li>IC IALLUIS and IC IALLU are always <b>UNDEFINED</b> at EL0 using AArch64.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Execution of the specified instructions is trapped to EL2, when EL2 is enabled in the current Security state.</p>	x

Bits	Name	Description	Reset
[23]	TPCP	<p>Trap data or unified cache maintenance instructions that operate to the Point of Coherency or Persistence. Traps execution of those cache maintenance instructions to EL2, when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>If EL0 is using AArch64 state and the value of AArch64-SCTLR_EL1.UCI is not 0, the following instructions are trapped to EL2 and reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>DC CIVAC, DC CVAC, DC CVAP. If the value of AArch64-SCTLR_EL1.UCI is 0 these instructions are <b>UNDEFINED</b> at EL0 and any resulting exception is higher priority than this trap to EL2.</li> </ul> </li> <li>If EL1 is using AArch64 state, the following instructions are trapped to EL2 and reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>DC IVAC, DC CIVAC, DC CVAC, DC CVAP.</li> </ul> </li> </ul> <p>If FEAT_DPB2 is implemented, this trap also applies to DC CVADP.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>An exception generated because an instruction is <b>UNDEFINED</b> at EL0 is higher priority than this trap to EL2. In addition: <ul style="list-style-type: none"> <li>AArch64 instructions which invalidate by VA to the Point of Coherency are always <b>UNDEFINED</b> at EL0 using AArch64.</li> </ul> </li> <li>In Armv8.0 and Armv8.1, this field is named TPC. From Armv8.2, it is named TPCP.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Execution of the specified instructions is trapped to EL2, when EL2 is enabled in the current Security state.</p>	x
[22]	TSW	<p>Trap data or unified cache maintenance instructions that operate by Set/Way. Traps execution of those cache maintenance instructions at EL1 to EL2, when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>If EL1 is using AArch64 state, accesses to DC ISW, DC CSW, DC CISW are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>Note:</b></p> <p>An exception generated because an instruction is <b>UNDEFINED</b> at EL0 is higher priority than this trap to EL2, and these instructions are always <b>UNDEFINED</b> at EL0.</p> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Execution of the specified instructions is trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p>	x



Bits	Name	Description	Reset
[21]	TACR	<p>Trap Auxiliary Control Registers. Traps EL1 accesses to the Auxiliary Control Registers to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>If EL1 is using AArch64 state, accesses to AArch64-ACTLR_EL1 to EL2, are trapped to EL2 and reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL1 accesses to the specified registers are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p> <p>AArch64-ACTLR_EL1 is not accessible at EL0.</p> <p>The Auxiliary Control Registers are <b>IMPLEMENTATION DEFINED</b> registers that might implement global control bits for the PE.</p>	x
[20]	TIDCP	<p>Trap IMPLEMENTATION DEFINED functionality. Traps EL1 accesses to the encodings reserved for IMPLEMENTATION DEFINED functionality to EL2, when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, access to any of the encodings in the following reserved encoding spaces are trapped and reported using EC syndrome 0x18: <ul style="list-style-type: none"> <li>IMPLEMENTATION DEFINED System instructions, which are accessed using SYS and SYSL, with CRn == {11, 15}.</li> <li>IMPLEMENTATION DEFINED System registers, which are accessed using MRS and MSR with the S3_&lt;op1&gt;_&lt;Cn&gt;_&lt;Cm&gt;_&lt;op2&gt; register name.</li> </ul> </li> </ul> <p>When this functionality is accessed from EL0:</p> <ul style="list-style-type: none"> <li>If HCR_EL2.TIDCP is 1, it is IMPLEMENTATION DEFINED whether any accesses from EL0 are trapped to EL2. In this implementation, such accesses are not trapped to EL2.</li> <li>If HCR_EL2.TIDCP is 0, any accesses from EL0 are <b>UNDEFINED</b> and generate an exception that is taken to EL1 or EL2.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL1 accesses to or execution of the specified encodings reserved for <b>IMPLEMENTATION DEFINED</b> functionality are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>An implementation can also include IMPLEMENTATION DEFINED registers that provide additional controls, to give finer-grained control of the trapping of IMPLEMENTATION DEFINED features.</p> <p>The trapping of accesses to these registers from EL1 is higher priority than an exception resulting from the register access being <b>UNDEFINED</b>.</p>	x
[19]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[18]	TID3	<p>Trap ID group 3. Traps EL1 reads of group 3 ID registers to EL2, when EL2 is enabled in the current Security state, as follows:</p> <p>In AArch64 state:</p> <ul style="list-style-type: none"> <li>Reads of the following registers are trapped to EL2, reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-ID_PFR0_EL1, AArch64-ID_PFR1_EL1, AArch64-ID_PFR2_EL1, AArch64-ID_DFR0_EL1, AArch64-ID_AFR0_EL1, AArch64-ID_MMFR0_EL1, AArch64-ID_MMFR1_EL1, AArch64-ID_MMFR2_EL1, AArch64-ID_MMFR3_EL1, AArch64-ID_ISAR0_EL1, AArch64-ID_ISAR1_EL1, AArch64-ID_ISAR2_EL1, AArch64-ID_ISAR3_EL1, AArch64-ID_ISAR4_EL1, AArch64-ID_ISAR5_EL1, AArch64-MVFR0_EL1, AArch64-MVFR1_EL1, AArch64-MVFR2_EL1.</li> <li>AArch64-ID_AA64PFR0_EL1, AArch64-ID_AA64PFR1_EL1, AArch64-ID_AA64DFR0_EL1, AArch64-ID_AA64DFR1_EL1, AArch64-ID_AA64ISAR0_EL1, AArch64-ID_AA64ISAR1_EL1, AArch64-ID_AA64MMFR0_EL1, AArch64-ID_AA64MMFR1_EL1, AArch64-ID_AA64AFR0_EL1, AArch64-ID_AA64AFR1_EL1.</li> <li>AArch64-ID_MMFR4_EL1.</li> <li>AArch64-ID_AA64MMFR2_EL1, AArch64-ID_ISAR6_EL1.</li> <li>Otherwise, it is <b>IMPLEMENTATION DEFINED</b> whether this field traps MRS accesses to registers in the following range that are not already mentioned in this field description: Op0 == 3, op1 == 0, CRn == c0, CRm == {c2-c7}, op2 == {0-7}. In this implementation, this field does not trap such accesses.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>The specified EL1 read accesses to ID group 3 registers are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p>	x
[17]	TID2	<p>Trap ID group 2. Traps the following register accesses to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>If EL1 is using AArch64, reads of AArch64-CTR_ELO, AArch64-CCSIDR_EL1, AArch64-CCSIDR2_EL1, AArch64-CLIDR_EL1, and AArch64-CSSELR_EL1 are trapped to EL2, reported using EC syndrome value 0x18.</li> <li>If ELO is using AArch64 and the value of AArch64-SCTLR_EL1.UCT is not 0, reads of AArch64-CTR_ELO are trapped to EL2, reported using EC syndrome value 0x18. If the value of AArch64-SCTLR_EL1.UCT is 0, then ELO reads of AArch64-CTR_ELO are trapped to EL1 and the resulting exception takes precedence over this trap.</li> <li>If EL1 is using AArch64, writes to AArch64-CSSELR_EL1 are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>The specified EL1 and ELO accesses to ID group 2 registers are trapped to EL2, when EL2 is enabled in the current Security state.</p>	x

Bits	Name	Description	Reset
[16]	TID1	<p>Trap ID group 1. Traps EL1 reads of the following registers to EL2, when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>Accesses of AArch64-MPUIR_EL1, AArch64-REVIDR_EL1, AArch64-AIDR_EL1, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>The specified EL1 read accesses to ID group 1 registers are trapped to EL2, when EL2 is enabled in the current Security state.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p>	x
[15]	RES0	Reserved	RES0
[14]	TWE	<p>Traps EL0 and EL1 execution of WFE instructions to EL2, when EL2 is enabled in the current Security state, from both Execution states, reported using EC syndrome value 0x01.</p> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Any attempt to execute a WFE instruction at EL0 or EL1 is trapped to EL2, when EL2 is enabled in the current Security state, if the instruction would otherwise have caused the PE to enter a low-power state and it is not trapped by AArch32-SCTLR.nTWE or AArch64-SCTLR_EL1.nTWE.</p> <p><b>Note:</b></p> <p>Since a WFE can complete at any time, even without a Wakeup event, the traps on WFE are not guaranteed to be taken, even if the WFE is executed when there is no Wakeup event. The only guarantee is that if the instruction does not complete in finite time in the absence of a Wakeup event, the trap will be taken.</p> <p>For more information about when WFE instructions can cause the PE to enter a low-power state, see <i>Wait for Event mechanism and Send event</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x
[13]	TWI	<p>Traps EL0 and EL1 execution of WFI instructions to EL2, when EL2 is enabled in the current Security state, from both Execution states, reported using EC syndrome value 0x01.</p> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Any attempt to execute a WFI instruction at EL0 or EL1 is trapped to EL2, when EL2 is enabled in the current Security state, if the instruction would otherwise have caused the PE to enter a low-power state and it is not trapped by AArch32-SCTLR.nTWI or AArch64-SCTLR_EL1.nTWI.</p> <p><b>Note:</b></p> <p>Since a WFI can complete at any time, even without a Wakeup event, the traps on WFI are not guaranteed to be taken, even if the WFI is executed when there is no Wakeup event. The only guarantee is that if the instruction does not complete in finite time in the absence of a Wakeup event, the trap will be taken.</p> <p>For more information about when WFI instructions can cause the PE to enter a low-power state, see <i>Wait for Interrupt</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x

Bits	Name	Description	Reset
[12]	DC	<p>Default Cacheability.</p> <p><b>0b0</b></p> <p>This control has no effect on the EL1&amp;O translation regime.</p> <p><b>0b1</b></p> <p>In both Security states:</p> <ul style="list-style-type: none"> <li>When EL1 is using AArch64, the PE behaves as if the value of the AArch64-SCTLR_EL1.M field is 0 for all purposes other than returning the value of a direct read of AArch64-SCTLR_EL1.</li> <li>If stage 1 EL1&amp;O translation regime is in PMSAv8-64 context, the PE behaves as if the value of the AArch64-SCTLR_EL1.BR field is 0 for all purposes other than returning the value of a direct read of AArch64-SCTLR_EL1.</li> <li>The PE behaves as if the value of the HCR_EL2.VM field is 1 for all purposes other than returning the value of a direct read of HCR_EL2.</li> <li>The memory type produced by stage 1 of the EL1&amp;O translation regime is Normal Non-Shareable, Inner Write-Back Read-Allocate Write-Allocate, Outer Write-Back Read-Allocate Write-Allocate.</li> </ul> <p>This field has no effect on the EL2 translation regime.</p> <p>This bit is permitted to be cached in a TLB.</p>	x
[11:10]	BSU	<p>Barrier Shareability upgrade. This field determines the minimum shareability domain that is applied to any barrier instruction executed from EL1 or EL0:</p> <p><b>0b00</b></p> <p>No effect.</p> <p><b>0b01</b></p> <p>Inner Shareable.</p> <p><b>0b10</b></p> <p>Outer Shareable.</p> <p><b>0b11</b></p> <p>Full system.</p> <p>This value is combined with the specified level of the barrier held in its instruction, using the same principles as combining the shareability attributes from two stages of address translation.</p>	xx
[9]	FB	<p>Force broadcast. Causes the following instructions to be broadcast within the Inner Shareable domain when executed from EL1:</p> <p>AArch64: TLBI VMALLE1, TLBI VAE1, TLBI ASIDE1, TLBI VAAE1, TLBI VALE1, TLBI VAALE1, IC IALLU, TLBI RVAE1, TLBI RVAAE1, TLBI RVALE1, TLBI RVAALE1.</p> <p><b>0b0</b></p> <p>This field has no effect on the operation of the specified instructions.</p> <p><b>0b1</b></p> <p>When one of the specified instruction is executed at EL1, the instruction is broadcast within the Inner Shareable shareability domain.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p>	x

Bits	Name	Description	Reset
[8]	VSE	<p>Virtual SError interrupt.</p> <p><b>0b0</b></p> <p>This mechanism is not making a virtual SError interrupt pending.</p> <p><b>0b1</b></p> <p>A virtual SError interrupt is pending because of this mechanism.</p> <p>The virtual SError interrupt is enabled only when the value of HCR_EL2.{TGE, AMO} is {0, 1}.</p>	x
[7]	VI	<p>Virtual IRQ Interrupt.</p> <p><b>0b0</b></p> <p>This mechanism is not making a virtual IRQ pending.</p> <p><b>0b1</b></p> <p>A virtual IRQ is pending because of this mechanism.</p> <p>The virtual IRQ is enabled only when the value of HCR_EL2.{TGE, IMO} is {0, 1}.</p>	x
[6]	VF	<p>Virtual FIQ Interrupt.</p> <p><b>0b0</b></p> <p>This mechanism is not making a virtual FIQ pending.</p> <p><b>0b1</b></p> <p>A virtual FIQ is pending because of this mechanism.</p> <p>The virtual FIQ is enabled only when the value of HCR_EL2.{TGE, FMO} is {0, 1}.</p>	x
[5]	AMO	<p>Physical SError interrupt routing.</p> <p><b>0b0</b></p> <p>When executing at Exception levels below EL2, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>When the value of HCR_EL2.TGE is 0, Physical SError interrupts are not taken to EL2.</li> <li>When the value of HCR_EL2.TGE is 1, Physical SError interrupts are taken to EL2.</li> <li>Virtual SError interrupts are disabled.</li> </ul> <p><b>0b1</b></p> <p>When executing at any Exception level, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>Physical SError interrupts are taken to EL2.</li> <li>When the value of HCR_EL2.TGE is 0, then virtual SError interrupts are enabled.</li> </ul> <p>If EL2 is enabled in the current Security state and the value of HCR_EL2.TGE is 1:</p> <ul style="list-style-type: none"> <li>Regardless of the value of the AMO bit physical asynchronous External aborts and SError interrupts target EL2.</li> <li>This field behaves as 1 for all purposes other than a direct read of the value of this bit.</li> </ul> <p>For more information, see <i>Asynchronous exception routing</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x

Bits	Name	Description	Reset
[4]	IMO	<p>Physical IRQ Routing.</p> <p><b>0b0</b></p> <p>When executing at Exception levels below EL2, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>When the value of HCR_EL2.TGE is 0, Physical IRQ interrupts are not taken to EL2.</li> <li>When the value of HCR_EL2.TGE is 1, Physical IRQ interrupts are taken to EL2 unless they are routed to EL3.</li> <li>Virtual IRQ interrupts are disabled.</li> </ul> <p><b>0b1</b></p> <p>When executing at any Exception level, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>Physical IRQ interrupts are taken to EL2, unless they are routed to EL3.</li> <li>When the value of HCR_EL2.TGE is 0, then Virtual IRQ interrupts are enabled.</li> </ul> <p>If EL2 is enabled in the current Security state, and the value of HCR_EL2.TGE is 1:</p> <ul style="list-style-type: none"> <li>Regardless of the value of the IMO bit, physical IRQ Interrupts target EL2.</li> <li>This field behaves as 1 for all purposes other than a direct read of the value of this bit.</li> </ul> <p>For more information, see <i>Asynchronous exception routing</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x
[3]	FMO	<p>Physical FIQ Routing.</p> <p><b>0b0</b></p> <p>When executing at Exception levels below EL2, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>When the value of HCR_EL2.TGE is 0, Physical FIQ interrupts are not taken to EL2.</li> <li>When the value of HCR_EL2.TGE is 1, Physical FIQ interrupts are taken to EL2.</li> <li>Virtual FIQ interrupts are disabled.</li> </ul> <p><b>0b1</b></p> <p>When executing at any Exception level, and EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>Physical FIQ interrupts are taken to EL2.</li> <li>When HCR_EL2.TGE is 0, then Virtual FIQ interrupts are enabled.</li> </ul> <p>If EL2 is enabled in the current Security state and the value of HCR_EL2.TGE is 1:</p> <ul style="list-style-type: none"> <li>Regardless of the value of the FMO bit, physical FIQ Interrupts target EL2.</li> <li>This field behaves as 1 for all purposes other than a direct read of the value of this bit.</li> </ul> <p>For more information, see <i>Asynchronous exception routing</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x

Bits	Name	Description	Reset
[2]	PTW	<p>Protected Table Walk. In the EL1&amp;O translation regime, a translation table access made as part of a stage 1 translation table walk is subject to a stage 2 translation. The combining of the memory type attributes from the two stages of translation means the access might be made to a type of Device memory. If this occurs, then the value of this bit determines the behavior:</p> <p><b>0b0</b></p> <p>The translation table walk occurs as if it is to Normal Non-cacheable memory. This means it can be made speculatively.</p> <p><b>0b1</b></p> <p>The memory access generates a stage 2 Permission fault.</p> <p>This bit is permitted to be cached in a TLB.</p> <p>When HCR_EL2.TGE is 1, the PE ignores the value of this field for all purposes other than a direct read of this field.</p> <p>In a PMSA-only implementation, this bit is permitted to be <b>RES0</b>.</p>	x
[1]	<b>RES1</b>	Reserved	<b>RES1</b>
[0]	VM	<p>Virtualization enable. Enables stage 2 address translation for the EL1&amp;O translation regime, when EL2 is enabled in the current Security state.</p> <p><b>0b0</b></p> <p>EL1&amp;O stage 2 address translation disabled.</p> <p><b>0b1</b></p> <p>EL1&amp;O stage 2 address translation enabled.</p> <p>If HCR_EL2.VM is 1 and SCTLR_EL2.{M, BR} is {0, 0}, then the memory attribute becomes <b>UNKNOWN</b>.</p> <p>When the value of this bit is 1, data cache invalidate instructions executed at EL1 perform a data cache clean and invalidate. For the invalidate by set/way instruction this behavior applies regardless of the value of the HCR_EL2.SWIO bit.</p> <p>This bit is permitted to be cached in a TLB.</p>	x

## Access

MRS <Xt>, HCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b000

MSR HCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b000

## Accessibility

MRS <Xt>, HCR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = HCR_EL2;
```

MSR HCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    HCR_EL2 = X[t, 64];
```

A.2.2.85 CPTR\_EL2, Architectural Feature Trap Register (EL2)

Controls trapping to EL2 of accesses to AArch64-CPACR\_EL1, trace, and Advanced SIMD and floating-point functionality.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

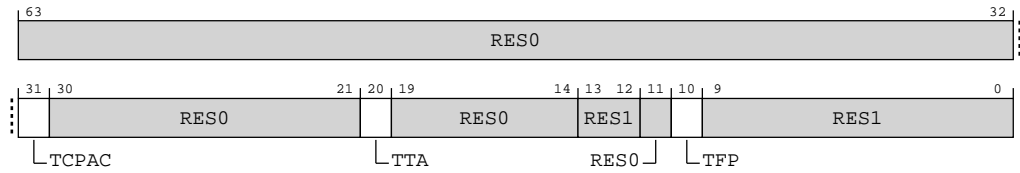


Where the reset reads xxxx, see individual bits.

Bit descriptions

This format applies in all Armv8.0 implementations.



**Figure A-145: AARCH64\_CPTR\_EL2 bit assignments****Table A-375: CPTR\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	TCPAC	<p>In AArch64 state, traps accesses to AArch64-CPACR_EL1 from EL1 to EL2, when EL2 is enabled in the current Security state. The exception is reported using ESR_ELx.EC value 0x18.</p> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL1 accesses to the following registers are trapped to EL2, when EL2 is enabled in the current Security state:</p> <ul style="list-style-type: none"> <li>AArch64-CPACR_EL1.</li> </ul> <p>When AArch64-HCR_EL2.TGE is 1, this control does not cause any instructions to be trapped.</p> <p><b>Note:</b> AArch64-CPACR_EL1 is not accessible at ELO.</p>	x
[30:21]	RES0	Reserved	RES0
[20]	TTA	<p>Traps System register accesses to all implemented trace registers from both Execution states to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to trace registers with op0=2, op1=1, and CRn&lt;0b1000 are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>Any attempt at ELO, EL1, or EL2, to execute a System register access to an implemented trace register is trapped to EL2, when EL2 is enabled in the current Security state, unless it is trapped by one of the following controls:</p> <ul style="list-style-type: none"> <li>AArch64-CPACR_EL1.TTA.</li> <li>The ETMv4 architecture does not permit ELO to access the trace registers. If the trace unit implements FEAT_ETMv4, ELO accesses to the trace registers are UNDEFINED, and any resulting exception is higher priority than an exception that would be generated because the value of AArch64-CPTR_EL2.TTA is 1.</li> <li>EL2 does not provide traps on trace register accesses through the optional memory-mapped interface.</li> </ul> <p>System register accesses to the trace registers can have side-effects. When a System register access is trapped, any side-effects that are normally associated with the access do not occur before the exception is taken.</p> <p>If System register access to the trace functionality is not supported, this bit is <b>RES0</b>.</p>	x

Bits	Name	Description	Reset
[19:14]	RES0	Reserved	RES0
[13:12]	RES1	Reserved	RES1
[11]	RES0	Reserved	RES0
[10]	TFP	Traps execution of instructions which access the Advanced SIMD and floating-point functionality, from both Execution states to EL2, when EL2 is enabled in the current Security state, as follows: <ul style="list-style-type: none"><li>In AArch64 state, accesses to the following registers are trapped to EL2, reported using ESR_ELx.EC value 0x07:<ul style="list-style-type: none"><li>AArch64-FPCR, AArch64-FPSR, AArch64-FPEXC32_EL2, any of the SIMD and floating-point registers V0-V31, including their views as D0-D31 registers or S0-S31 registers.</li></ul></li></ul> <p><b>0b0</b></p> <p>This control does not cause execution of any instructions to be trapped.</p> <p><b>0b1</b></p> <p>This control causes execution of these instructions at EL2, EL1, and EL0 to be trapped.</p> <p>AArch64-FPEXC32_EL2 is not accessible from EL0 using AArch64.</p>	x
[9:0]	RES1	Reserved	RES1

Access

MRS <Xt>, CPTR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b010

MSR CPTR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b010

Accessibility

MRS <Xt>, CPTR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = CPTR_EL2;
```

MSR CPTR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    CPTR_EL2 = X[t, 64];
```

A.2.2.86 HACR\_EL2, Hypervisor Auxiliary Control Register

Controls trapping to EL2 of **IMPLEMENTATION DEFINED** aspects of EL1 or ELO operation.

Configurations

This register is available in all configurations.

Attributes

Width

64

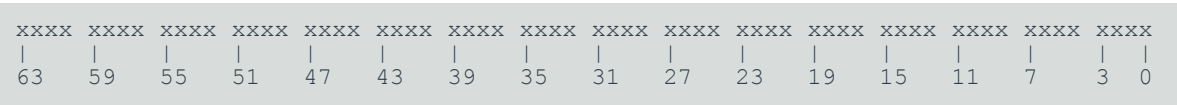
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-146: AARCH64\_HACR\_EL2 bit assignments

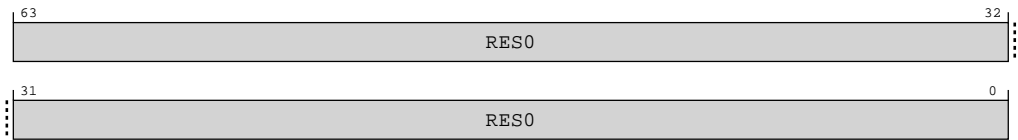


Table A-378: HACR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, HACR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b111

MSR HACR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b111

Accessibility

MRS <Xt>, HACR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = HACR_EL2;
```

MSR HACR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    HACR_EL2 = X[t, 64];
```

A.2.2.87 VSCTLR\_EL2, Virtualization System Control Register (EL2)

Provides configuration information for VMSAv8-64 and PMSAv8-64 virtualization using stage 2 of EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

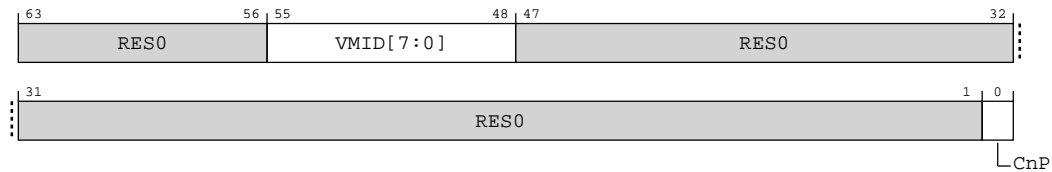
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-147: AARCH64\_VSCTLR\_EL2 bit assignments**



**Table A-381: VSCTLR\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:48]	VMID[7:0]	The VMID for the EL1-Guest-OS.	8 {x}
[47:1]	RES0	Reserved	RES0
[0]	CnP	<p><b>When AArch64-VTCR_EL2.MSA == '1'</b></p> <p>Common not Private. This bit indicates whether stage 2 of EL1&amp;O translations are a member of a common set that can be used by every PE in the Inner Shareable domain for which the value of VSCTLR_EL2.CnP is 1.</p> <p><b>0b0</b></p> <p>The stage 2 translations of the EL1&amp;O translation regime are permitted to differ in other PEs in the Inner Shareable domain. This is not affected by the value of the current VMID.</p> <p><b>0b1</b></p> <p>The stage 2 translations of the EL1&amp;O translation regime are the same for every other PE in the Inner Shareable domain for which the value of VSCTLR_EL2.CnP is 1 and the VMID is the same as the current VMID.</p> <p>If the value of VSCTLR_EL2.CnP bit is 1 on multiple PEs in the same Inner Shareable domain and the stage 2 EL1&amp;O translation does not point to the same configurations when using the current VMID, then the results of the translations are <b>CONSTRAINED UNPREDICTABLE</b>, see <i>CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a></i>.</p> <p>In an implementation that does not support VMSAv8-64 at stage 1 EL1&amp;O translation regime this field is <b>RES0</b>.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxxx

## Access

MRS &lt;Xt&gt;, VSCTLR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0000	0b000

MSR VSCTLR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0000	0b000

Accessibility

MRS <Xt>, VSCTLR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VSCTLR_EL2;
```

MSR VSCTLR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VSCTLR_EL2 = X[t, 64];
```

A.2.2.88 TCR\_EL2, Translation Control Register (EL2)

This register controls stage 1 of the EL2 translation regime, that supports a single VA range, translated using AArch64-TTBR0\_EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

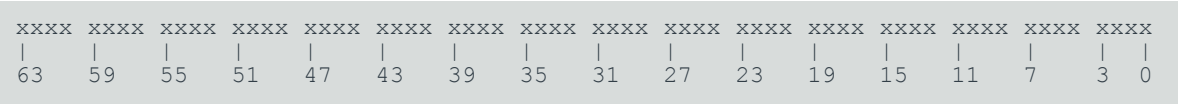
Functional group

Generic System Control

Access type

See bit descriptions

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Any of the bits in TCR\_EL2 are permitted to be cached in a TLB.

Figure A-148: AARCH64\_TCR\_EL2 bit assignments

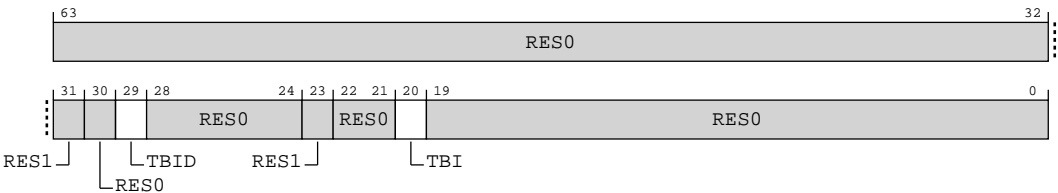


Table A-384: TCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	RES1	Reserved	RES1
[30]	RES0	Reserved	RES0
[29]	TBID	Controls the use of the top byte of instruction addresses for address matching.  For the purpose of this field, all cache maintenance and address translation instructions that perform address translation are treated as data accesses.  For more information, see <i>Address tagging</i> in the <i>Arm® Architecture Reference Manual for A-profile architecture</i> .  <b>0b0</b> TCR_EL2.TBI applies to Instruction and Data accesses.  <b>0b1</b> TCR_EL2.TBI applies to Data accesses only.  This affects addresses where the address would be translated by EL2 MPU.	x
[28:24]	RES0	Reserved	RES0
[23]	RES1	Reserved	RES1
[22:21]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[20]	TBI	<p>Top Byte ignored. Indicates whether the top byte of an address is used for address match for the EL2 MPU regions, or ignored and used for tagged addresses.</p> <p>For more information, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b0</b> Top Byte used in the address calculation.</p> <p><b>0b1</b> Top Byte ignored in the address calculation.</p> <p>This affects addresses generated in EL2 using AArch64 where the address would be translated by the EL2 MPU. It has an effect whether the EL2 translation regime is enabled or not.</p> <p>If FEAT_PAuth is implemented and TCR_EL2.TBID is 1, then this field only applies to Data accesses.</p> <p>If the value of TBI is 1, then bits[63:56] of that target address are also set to 0 before the address is stored in the PC, in the following cases:</p> <ul style="list-style-type: none"> <li>• A branch or procedure return within EL2.</li> <li>• An exception taken to EL2.</li> <li>• An exception return to EL2.</li> </ul>	x
[19:0]	RES0	Reserved	RES0

## Access

MRS <Xt>, TCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0000	0b010

MSR TCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0000	0b010

## Accessibility

MRS <Xt>, TCR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = TCR_EL2;

```

MSR TCR\_EL2, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then

```



```
TCR_EL2 = X[t, 64];
```

A.2.2.89 VTCR\_EL2, Virtualization Translation Control Register

The control register for stage 2 of the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Any of the bits in VTCR\_EL2 are permitted to be cached in a TLB.

Figure A-149: AARCH64\_VTCR\_EL2 bit assignments

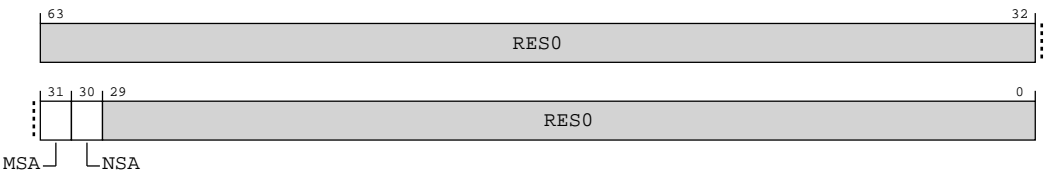


Table A-387: VTCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31]	MSA	<b>When AArch64-ID_AA64MMFR0_EL1.MSA_frac == '0010'</b> Stage 1 EL1&0 translation regime memory system architecture. <b>0b0</b> Stage 1 EL1&0 translation regime uses PMSAv8-64 memory architecture. <b>0b1</b> Stage 1 EL1&0 translation regime uses VMSAv8-64 memory architecture.  <b>When AArch64-ID_AA64MMFR0_EL1.MSA_frac == '0001'</b> RES1 <b>Otherwise</b> RES1	x
[30]	NSA	Non-secure stage 2 translation output address space. <b>0b0</b> All stage 2 translations for the Non-secure PA space of the Secure EL1&0 translation regime access the Secure PA space. <b>0b1</b> All stage 2 translations for the Non-secure PA space of the Secure EL1&0 translation regime access the Non-secure PA space.  This bit behaves as 1 for all purposes other than reading back the value of the bit when the value of AArch64-VSTCR_EL2.SA is 1.	x
[29:0]	RES0	Reserved	RES0

## Access

Unless stated otherwise, any of the bits in VTCR\_EL2 are permitted to be cached in a TLB.

MRS <Xt>, VTCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b010

MSR VTCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b010

## Accessibility

Unless stated otherwise, any of the bits in VTCR\_EL2 are permitted to be cached in a TLB.

MRS <Xt>, VTCR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = VTCR_EL2;

```

MSR VTCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VTCR_EL2 = X[t, 64];
```

A.2.2.90 VSTCR\_EL2, Virtualization Secure Translation Control Register

The control register for stage 2 of the Secure EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



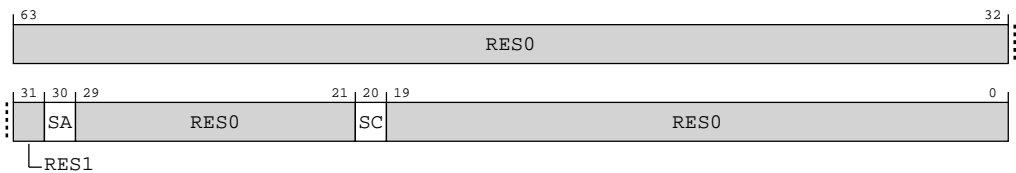
Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Any of the bits in VSTCR\_EL2 are permitted to be cached in a TLB.

Figure A-150: AARCH64\_VSTCR\_EL2 bit assignments



**Table A-390: VSTCR\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	RES1	Reserved	RES1
[30]	SA	Secure stage 2 translation output address space.  <b>0b0</b> All stage 2 translations for the Secure PA space access the Secure PA space.  <b>0b1</b> All stage 2 translations for the Secure PA space access the Non-secure PA space.	x
[29:21]	RES0	Reserved	RES0
[20]	SC	NS check enable bit.  <b>0b0</b> Least secure NS configuration is selected from the stage 1 and stage 2 EL1&0 translation regime for the given address.  <b>0b1</b> Stage 2 NS configuration is checked against stage 1 NS configuration in EL1&0 translation regime for the given address, and generate a fault if they are different.	x
[19:0]	RES0	Reserved	RES0

### Access

MRS &lt;Xt&gt;, VSTCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0110	0b010

MSR VSTCR\_EL2, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0110	0b010

### Accessibility

MRS &lt;Xt&gt;, VSTCR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = VSTCR_EL2;

```

MSR VSTCR\_EL2, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    VSTCR_EL2 = X[t, 64];

```

A.2.2.91 AFSRO\_EL2, Auxiliary Fault Status Register 0 (EL2)

Provides additional implementation defined fault status information for Data Abort, Instruction Abort or SError interrupt taken to EL2

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-151: AARCH64\_AFSRO\_EL2 bit assignments

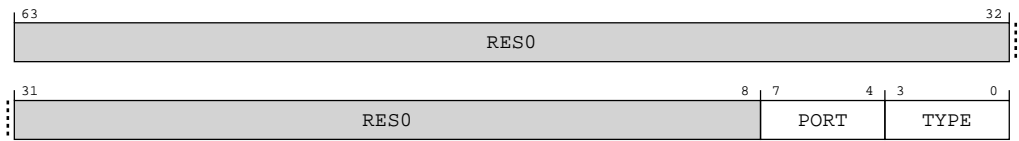


Table A-393: AFSRO\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	PORT	<p>Memory or bus interface that caused the abort.</p> <p><b>0b0000</b> MM. Main Manager port.</p> <p><b>0b0001</b> LLRAM. Low-Latency RAM port.</p> <p><b>0b0010</b> LLPP. Low-Latency Peripheral Port.</p> <p><b>0b0011</b> SPP. Shared Peripheral Port.</p> <p><b>0b0100</b> ITCM. Instruction Tightly Coupled Memory.</p> <p><b>0b0101</b> DTCM. Data Tightly Coupled Memory.</p> <p><b>0b0110</b> Overlapping or illegal port. Used for accesses that target multiple ports, when they simultaneously belong in two or more of the ITCM, DTCM, LLRAM, LLPP or SPP enabled regions. Also used for page table accesses if they belong in any of the ITCM, DTCM, LLRAM, LLPP or SPP enabled regions.</p> <p><b>0b0111</b> Unknown. All faults other than Instruction or Data aborts will have this type. For External aborts and Unsupported Exclusive or Atomic access faults, this is used for ambiguous memory accesses or for faults that do not have an associated address. For other Instruction or Data aborts, this indicates that the port information is not applicable to the fault.</p> <p><b>0b1000</b> SEI. System abort signaled by System Error Interrupt input pins.</p> <p>Other values are Reserved.</p>	xxxx
[3:0]	TYPE	<p>Fault type.</p> <p><b>0b0000</b> Error on data.</p> <p><b>0b0001</b> Timeout error.</p> <p><b>0b0010</b> Error on interrupt latency. Indicates the abort was generated by an instruction trapped by AArch64-IMP_INTLATENCY_EL2 controls.</p> <p><b>0b0011</b> Other error.</p> <p>Other values are Reserved.</p>	xxxx

## Access

MRS <Xt>, AFSRO\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0001	0b000

MSR AFSRO\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0001	0b000

Accessibility

MRS <Xt>, AFSRO\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = AFSRO_EL2;
```

MSR AFSRO\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AFSRO_EL2 = X[t, 64];
```

A.2.2.92 AFSR1\_EL2, Auxiliary Fault Status Register 1 (EL2)

Provides additional **IMPLEMENTATION DEFINED** fault status information for exceptions taken to EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-152: AARCH64\_AFSR1\_EL2 bit assignments

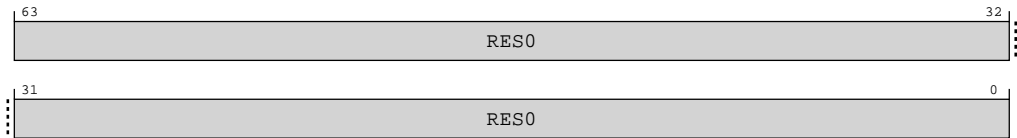


Table A-396: AFSR1\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, AFSR1\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0001	0b001

MSR AFSR1\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0001	0b001

Accessibility

MRS <Xt>, AFSR1\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = AFSR1_EL2;
```

MSR AFSR1\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AFSR1_EL2 = X[t, 64];
```



A.2.2.93 ESR\_EL2, Exception Syndrome Register (EL2)

Holds syndrome information for an exception taken to EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

ESR\_EL2 is made **UNKNOWN** as a result of an exception return from EL2.

When an UNPREDICTABLE instruction is treated as UNDEFINED, and the exception is taken to EL2, the value of ESR\_EL2 is **UNKNOWN**. The value written to ESR\_EL2 must be consistent with a value that could be created as a result of an exception from the same Exception level that generated the exception as a result of a situation that is not UNPREDICTABLE at that Exception level, in order to avoid the possibility of a privilege violation.

Figure A-153: AARCH64\_ESR\_EL2 bit assignments

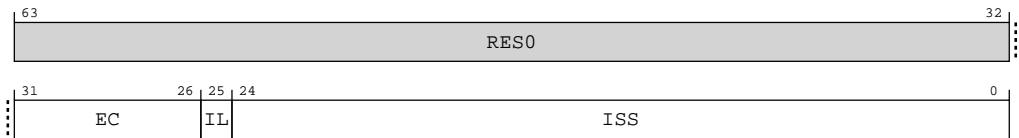


Table A-399: ESR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:26]	EC	<p>Exception Class. Indicates the reason for the exception that this register holds information about.</p> <p>For each EC value, the table references a subsection that gives information about:</p> <ul style="list-style-type: none"> <li>The cause of the exception, for example the configuration required to enable the trap.</li> <li>The encoding of the associated ISS.</li> </ul> <p>Possible values of the EC field are:</p>	6 {x}
[31:26 continued]	EC	<p><b>0b0000000</b> Unknown reason.</p> <p><b>0b0000001</b> Trapped WFI or WFE instruction execution.</p> <p>Conditional WFE and WFI instructions that fail their condition code check do not cause an exception.</p> <p><b>0b000111</b> Access to Advanced SIMD, or floating-point functionality trapped by AArch64-CPACR_EL1.FPEN, AArch64-CPTR_EL2.FPEN, or AArch64-CPTR_EL2.TFP control.</p> <p>Excludes exceptions resulting from AArch64-CPACR_EL1 when the value of AArch64-HCR_EL2.TGE is 1, or because Advanced SIMD and floating-point are not implemented. These are reported with EC value 0b000000.</p>	6 {x}
[31:26 continued]	EC	<p><b>0b001001</b> Trapped use of a Pointer authentication instruction because HCR_EL2.API == 0.</p> <p><b>0b001110</b> Illegal Execution state.</p> <p><b>0b010101</b> SVC instruction execution in AArch64 state.</p> <p><b>0b010110</b> HVC instruction execution in AArch64 state, when HVC is not disabled.</p> <p><b>0b011000</b> Trapped MSR, MRS or System instruction execution in AArch64 state, that is not reported using EC 0b000000, 0b000001 or 0b000111.</p> <p>This includes all instructions that cause exceptions that are part of the encoding space defined in 'System instruction class encoding overview', except for those exceptions reported using EC values 0b000000, 0b000001, or 0b000111.</p>	6 {x}

Bits	Name	Description	Reset
[31:26 continued]	EC	<p><b>0b011100</b> Exception from a Pointer Authentication instruction authentication failure</p> <p><b>0b100000</b> Instruction Abort from a lower Exception level.</p> <p>Used for MMU faults generated by instruction accesses and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100001</b> Instruction Abort taken without a change in Exception level.</p> <p>Used for MMU faults generated by instruction accesses and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p>	6{x}
[31:26 continued]	EC	<p><b>0b100010</b> PC alignment fault exception.</p> <p><b>0b100100</b> Data Abort from a lower Exception level.</p> <p>Used for MMU faults generated by data accesses, alignment faults other than those caused by Stack Pointer misalignment, and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100101</b> Data Abort without a change in Exception level.</p> <p>Used for MMU faults generated by data accesses, alignment faults other than those caused by Stack Pointer misalignment, and synchronous External aborts, including synchronous parity or ECC errors. Not used for debug related exceptions.</p> <p><b>0b100110</b> SP alignment fault exception.</p>	6{x}
[31:26 continued]	EC	<p><b>0b101111</b> SError interrupt.</p> <p><b>0b110000</b> Breakpoint exception from a lower Exception level.</p> <p><b>0b110001</b> Breakpoint exception taken without a change in Exception level.</p> <p><b>0b110010</b> Software Step exception from a lower Exception level.</p> <p><b>0b110011</b> Software Step exception taken without a change in Exception level.</p> <p><b>0b110100</b> Watchpoint from a lower Exception level.</p>	6{x}

Bits	Name	Description	Reset
[31:26 continued]	EC	<p><b>0b110101</b> Watchpoint exceptions without a change in Exception level.</p> <p><b>0b111100</b> BRK instruction execution in AArch64 state.</p> <p>All other EC values are reserved by Arm, and:</p> <ul style="list-style-type: none"> <li>Unused values in the range 0b000000 - 0b101100 (0x00 - 0x2C) are reserved for future use for synchronous exceptions.</li> <li>Unused values in the range 0b101101 - 0b111111 (0x2D - 0x3F) are reserved for future use, and might be used for synchronous or asynchronous exceptions.</li> </ul> <p>The effect of programming this field to a reserved value is that behavior is <b>CONSTRAINED UNPREDICTABLE</b>.</p>	6{x}
[25]	IL	<p>Instruction Length for synchronous exceptions. Possible values of this bit are:</p> <p><b>0b0</b> 16-bit instruction trapped.</p> <p><b>0b1</b> 32-bit instruction trapped. This value is also used when the exception is one of the following:</p> <ul style="list-style-type: none"> <li>An SError interrupt.</li> <li>An Instruction Abort exception.</li> <li>A PC alignment fault exception.</li> <li>An SP alignment fault exception.</li> <li>A Data Abort exception for which the value of the ISV bit is 0.</li> <li>An Illegal Execution state exception.</li> <li>Any debug exception except for Breakpoint instruction exceptions. For Breakpoint instruction exceptions, this bit has its standard meaning: <ul style="list-style-type: none"> <li>0b1: 32-bit A64 BRK instruction.</li> </ul> </li> <li>An exception reported using EC value 0b000000.</li> </ul>	x
[24:0]	ISS	<p><b>ISS encoding for exceptions with an unknown reason</b></p> <p><b>24:0</b> Reserved, <b>RES0</b>.</p> <p>When an exception is reported using this EC code the IL field is set to 1.</p> <p>This EC code is used for all exceptions that are not covered by any other EC value. This includes exceptions that are generated in the following situations:</p>	25{x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>The attempted execution of an instruction bit pattern that has no allocated instruction or that is not accessible at the current Exception level and Security state, including: <ul style="list-style-type: none"> <li>A read access using a System register pattern that is not allocated for reads or that does not permit reads at the current Exception level and Security state.</li> </ul> </li> </ul>	25{x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>A write access using a System register pattern that is not allocated for writes or that does not permit writes at the current Exception level and Security state.</li> <li>Instruction encodings that are unallocated.</li> <li>Instruction encodings for instructions or System registers that are not implemented in the implementation.</li> </ul>	25{x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>In Debug state, the attempted execution of an instruction bit pattern that is not accessible in Debug state.</li> <li>In Non-debug state, the attempted execution of an instruction bit pattern that is not accessible in Non-debug state.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>In an implementation that does not include Advanced SIMD and floating-point functionality, an attempted access to Advanced SIMD or floating-point functionality under conditions where that access would be permitted if that functionality was present. This includes the attempted execution of an Advanced SIMD or floating-point instruction, and attempted accesses to Advanced SIMD and floating-point System registers.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>Attempted execution of: <ul style="list-style-type: none"> <li>An HVC instruction when disabled by AArch64-HCR_EL2.HCD.</li> <li>An SMC instruction.</li> <li>An HLT instruction when disabled by ext-EDSCR.HDE.</li> </ul> </li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>Attempted execution of an MSR or MRS instruction to access AArch64-SP_ELO when the value of AArch64-SPSel.SP is 0.</li> <li>Attempted execution of an MSR or MRS instruction using a _EL12 register name.</li> </ul>	25 {x}
[24:0 continued]	ISS	<p>Attempted execution, in Debug state, of:</p> <ul style="list-style-type: none"> <li>A DCPS1 instruction when the value of AArch64-HCR_EL2.TGE is 1 and EL2 is disabled or not implemented in the current Security state.</li> <li>A DCPS2 instruction from EL1 or ELO when EL2 is disabled or not implemented in the current Security state.</li> <li>A DCPS3 instruction.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>An exception that is taken to EL2 because the value of AArch64-HCR_EL2.TGE is 1 that, if the value of AArch64-HCR_EL2.TGE was 0 would have been reported with an ESR_ELx.EC value of 0b000111.</li> </ul>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from a WF* instruction</b></p> <p><b>24</b></p> <p>Condition code valid.</p> <p><b>0b0</b></p> <p>The COND field is not valid.</p> <p><b>0b1</b></p> <p>The COND field is valid.</p>	25 {x}
[24:0 continued]	ISS	<p><b>23:20</b></p> <p>For exceptions taken from AArch64, this field is set to 0b1110.</p> <p><b>19:2</b></p> <p>Reserved, <b>RES0</b>.</p> <p><b>1:0</b></p> <p>Trapped instruction. Possible values of this bit are:</p> <p><b>0b00</b></p> <p>WFI trapped.</p> <p><b>0b01</b></p> <p>WFE trapped.</p>	25 {x}
[24:0 continued]	ISS	<p>The following fields describe configuration settings for generating this exception:</p> <ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.{nTWE, nTWI}.</li> <li>AArch64-HCR_EL2.{TWE, TWI}.</li> </ul>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>ISS encoding for an exception from an access to SVE, Advanced SIMD or floating-point functionality, resulting from the FPEN and TFP traps</b> The accesses covered by this trap include: <ul style="list-style-type: none"> <li>• Execution of SVE or Advanced SIMD and floating-point instructions.</li> <li>• Accesses to the Advanced SIMD and floating-point System registers.</li> </ul>	25 {x}
[24:0 continued]	ISS	For an implementation that does not include either SVE or support for Advanced SIMD and floating-point, the exception is reported using the EC value 0b000000.	25 {x}
[24:0 continued]	ISS	<b>24</b> Condition code valid. <b>0b0</b> The COND field is not valid. <b>0b1</b> The COND field is valid.	25 {x}
[24:0 continued]	ISS	<b>23:20</b> For exceptions taken from AArch64, this field is set to 0b1110. <b>19:0</b> Reserved, <b>RES0</b> .	25 {x}
[24:0 continued]	ISS	The following fields describe the configuration settings for the traps that are reported using EC value 0b000111: <ul style="list-style-type: none"> <li>• AArch64-CPACR_EL1.FPEN, for accesses to SIMD and floating-point registers trapped to EL1.</li> <li>• AArch64-CPTR_EL2.FPEN and AArch64-CPTR_EL2.TFP, for accesses to SIMD and floating-point registers trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from an Illegal Execution state, or a PC or SP alignment fault</b> <b>24:0</b> Reserved, <b>RES0</b> . There are no configuration settings for generating Illegal Execution state exceptions and PC alignment fault exceptions. For more information about PC alignment fault exceptions, see <i>PC alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> . SP alignment checking in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> describes the configuration settings for generating SP alignment fault exceptions.	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from HVC or SVC instruction execution</b> <b>24:16</b> Reserved, <b>RES0</b> . For A64 instructions, see SVC in the and 'HVC'.	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from MSR, MRS, or System instruction execution in AArch64 state</b> <b>24:22</b> Reserved, <b>RES0</b> . <b>21:20</b> The Op0 value from the issued instruction. <b>19:17</b> The Op2 value from the issued instruction.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>16:14</b> The Op1 value from the issued instruction.  <b>13:10</b> The CRn value from the issued instruction.  <b>9:5</b> The Rt value from the issued instruction, the general-purpose register used for the transfer.	25 {x}
[24:0 continued]	ISS	<b>4:1</b> The CRm value from the issued instruction.  <b>0</b> Indicates the direction of the trapped instruction. <b>0b0</b> Write access, including MSR instructions. <b>0b1</b> Read access, including MRS instructions.	25 {x}
[24:0 continued]	ISS	For exceptions caused by System instructions, see <i>System instructions' subsection of 'Branches, exception generating and System instructions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> for the encoding values returned by an instruction.  The following fields describe configuration settings for generating the exception that is reported using EC value 0b011000:	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.UCI, for execution of cache maintenance instructions using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-SCTLR_EL1.UCT, for accesses to AArch64-CTR_EL0 using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-SCTLR_EL1.DZE, for execution of DC ZVA instructions using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-SCTLR_EL1.UMA, for accesses to the PSTATE interrupt masks using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-CPACR_EL1.TTA, for accesses to the trace registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.TDCC, for accesses to the Debug Communications Channel (DCC) registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-CNTKCTL_EL1.{ELOPTEN, EL0VTEN, EL0PCTEN, EL0VCTEN} accesses to the Generic Timer registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> <li>AArch64-PMUSERENR_EL0.{ER, CR, SW, EN}, for accesses to the Performance Monitor registers using AArch64 state, MSR or MRS access trapped to EL1 or EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.{TRVM, TVM}, for accesses to virtual memory control registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TDZ, for execution of DC ZVA instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TTLB, for execution of TLB maintenance instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.{TSW, TPC, TPU}, for execution of cache maintenance instructions using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TACR, for accesses to the Auxiliary Control Register, AArch64-ACTLR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.TIDCP, for accesses to lockdown, DMA, and TCM operations using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.{TID1, TID2, TID3}, for accesses to ID group 1, ID group 2 or ID group 3 registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-CPTR_EL2.TCPAC, for accesses to AArch64-CPACR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-CPTR_EL2.TTA, for accesses to the trace registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-MDCR_EL2.TTRF, for accesses to the trace filter control register, AArch64-TRFCR_EL1, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TDRA, for accesses to Debug ROM registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TDOSA, for accesses to powerdown debug registers using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-CNTHCTL_EL2.{EL1PCEN, EL1PCTEN}, for accesses to the Generic Timer registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.TDA, for accesses to debug registers using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-MDCR_EL2.{TPM, TPMCR}, for accesses to Performance Monitor registers, using AArch64 state, MSR or MRS access trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>AArch64-HCR_EL2.APK, for accesses to Pointer authentication key registers. using AArch64 state, MSR or MRS access trapped to EL2.</li> <li>AArch64-HCR_EL2.AT, for execution of AT S1E* instructions, using AArch64 state, MSR or MRS access, trapped to EL2.</li> <li>AArch64-HCR_EL2.{TERR, FIEN}, for accesses to RAS registers, using AArch64 state, MSR or MRS access, trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from an Instruction Abort</b> <b>24:13</b> Reserved, RES0.	25 {x}
[24:0 continued]	ISS	<b>12:11</b> Synchronous Error Type. When IFSC is 0b010000, describes the PE error state after taking the Instruction Abort exception. <b>0b00</b> Recoverable state (UER). <b>0b10</b> Uncontainable (UC). <b>0b11</b> Restartable state (UEO).	25 {x}



Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>10</b> FAR not Valid, for a synchronous External abort other than a synchronous External abort on a translation table walk. <b>0b0</b> FAR is valid. <b>0b1</b> FAR is not valid, and holds an UNKNOWN value.	25 {x}
[24:0 continued]	ISS	<b>9</b> External abort type. <b>0b0</b> No IMPLEMENTATION DEFINED classification of External aborts.	25 {x}
[24:0 continued]	ISS	<b>8</b> Reserved, <b>RES0</b> . <b>7</b> For a stage 2 fault, indicates whether the fault was a stage 2 fault on an access made for a stage 1 translation table walk:	25 {x}
[24:0 continued]	ISS	<b>0b0</b> Fault not on a stage 2 translation for a stage 1 translation table walk. <b>0b1</b> Fault on the stage 2 translation of an access for a stage 1 translation table walk.	25 {x}
[24:0 continued]	ISS	<b>6</b> Reserved, <b>RES0</b> .	25 {x}
[24:0 continued]	ISS	<b>5:0</b> Instruction Fault Status Code. <b>0b000000</b> Address size fault, level 0 of translation or translation table base register. <b>0b000001</b> Address size fault, level 1. <b>0b000010</b> Address size fault, level 2.	25 {x}
[24:0 continued]	ISS	<b>0b000011</b> Address size fault, level 3. <b>0b000100</b> Translation fault, level 0. <b>0b000101</b> Translation fault, level 1. <b>0b000110</b> Translation fault, level 2.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>0b000111</b> Translation fault, level 3.  <b>0b001001</b> Access flag fault, level 1.  <b>0b001010</b> Access flag fault, level 2.  <b>0b001011</b> Access flag fault, level 3.  <b>0b001100</b> Permission fault, level 0.	25 {x}
[24:0 continued]	ISS	<b>0b001101</b> Permission fault, level 1.  <b>0b001110</b> Permission fault, level 2.  <b>0b001111</b> Permission fault, level 3.  <b>0b010000</b> Synchronous External abort, not on translation table walk or hardware update of translation table.	25 {x}
[24:0 continued]	ISS	<b>0b010100</b> Synchronous External abort on translation table walk or hardware update of translation table, level 0.  <b>0b010101</b> Synchronous External abort on translation table walk or hardware update of translation table, level 1.	25 {x}
[24:0 continued]	ISS	<b>0b010110</b> Synchronous External abort on translation table walk or hardware update of translation table, level 2.  <b>0b010111</b> Synchronous External abort on translation table walk or hardware update of translation table, level 3.  <b>0b110000</b> TLB conflict abort.  <b>0b110001</b> Unsupported atomic hardware update fault.	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Data Abort</b>  <b>24</b> Instruction Syndrome Valid. Indicates whether the syndrome information in ISS[23:14] is valid.  <b>0b0</b> No valid instruction syndrome. ISS[23:14] are RES0.  <b>0b1</b> ISS[23:14] hold a valid instruction syndrome.  <b>13</b> Reserved, RES0.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>10</b> FAR not Valid, for a synchronous External abort other than a synchronous External abort on a translation table walk. <b>0b0</b> FAR is valid. <b>0b1</b> FAR is not valid, and holds an UNKNOWN value.	25 {x}
[24:0 continued]	ISS	<b>9</b> External abort type. <b>0b0</b> No IMPLEMENTATION DEFINED classification of External aborts.	25 {x}
[24:0 continued]	ISS	<b>8</b> Cache maintenance. Indicates whether the Data Abort came from a cache maintenance or address translation instruction: <b>0b0</b> The Data Abort was not generated by the execution of one of the System instructions identified in the description of value 1.	25 {x}
[24:0 continued]	ISS	<b>0b1</b> The Data Abort was generated by either the execution of a cache maintenance instruction or by a synchronous fault on the execution of an address translation instruction. The r[DC ZVA](AArch64-dc-zva), r[DC GVA](AArch64-dc-gva), and r[DC GZVA](AArch64-dc-gzva) instructions are not classified as cache maintenance instructions, and therefore their execution cannot cause this field to be set to 1.	25 {x}
[24:0 continued]	ISS	<b>7</b> For a stage 2 fault, indicates whether the fault was a stage 2 fault on an access made for a stage 1 translation table walk: <b>0b0</b> Fault not on a stage 2 translation for a stage 1 translation table walk. <b>0b1</b> Fault on the stage 2 translation of an access for a stage 1 translation table walk.	25 {x}
[24:0 continued]	ISS	<b>6</b> Write not Read. Indicates whether a synchronous abort was caused by an instruction writing to a memory location, or by an instruction reading from a memory location. <b>0b0</b> Abort caused by an instruction reading from a memory location. <b>0b1</b> Abort caused by an instruction writing to a memory location.	25 {x}
[24:0 continued]	ISS	<b>5:0</b> Data Fault Status Code. <b>0b000000</b> Address size fault, level 0 of translation or translation table base register.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>0b000001</b> Address size fault, level 1. <b>0b000010</b> Address size fault, level 2. <b>0b000011</b> Address size fault, level 3. <b>0b000100</b> Translation fault, level 0.	25 {x}
[24:0 continued]	ISS	<b>0b000101</b> Translation fault, level 1. <b>0b000110</b> Translation fault, level 2. <b>0b000111</b> Translation fault, level 3. <b>0b001001</b> Access flag fault, level 1.	25 {x}
[24:0 continued]	ISS	<b>0b001010</b> Access flag fault, level 2. <b>0b001011</b> Access flag fault, level 3. <b>0b001100</b> Permission fault, level 0. <b>0b001101</b> Permission fault, level 1.	25 {x}
[24:0 continued]	ISS	<b>0b001110</b> Permission fault, level 2. <b>0b001111</b> Permission fault, level 3. <b>0b010000</b> Synchronous External abort, not on translation table walk or hardware update of translation table. <b>0b010100</b> Synchronous External abort on translation table walk or hardware update of translation table, level 0.	25 {x}
[24:0 continued]	ISS	<b>0b010101</b> Synchronous External abort on translation table walk or hardware update of translation table, level 1. <b>0b010110</b> Synchronous External abort on translation table walk or hardware update of translation table, level 2. <b>0b010111</b> Synchronous External abort on translation table walk or hardware update of translation table, level 3. <b>0b100001</b> Alignment fault.	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>0b110000</b> TLB conflict abort.  <b>0b110001</b> Unsupported atomic hardware update fault.  <b>0b110100</b> IMPLEMENTATION DEFINED fault (Lockdown).  <b>0b110101</b> IMPLEMENTATION DEFINED fault (Unsupported Exclusive or Atomic access).	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an SError interrupt</b>  <b>24</b>  <b>IMPLEMENTATION DEFINED</b> syndrome.  <b>0b0</b>  Bits [23:0] of the ISS field holds the fields described in this encoding	25 {x}
[24:0 continued]	ISS	<b>0b1</b>  Bits [23:0] of the ISS field holds IMPLEMENTATION DEFINED syndrome information that can be used to provide additional information about the SError interrupt.	25 {x}
[24:0 continued]	ISS	<b>23:14</b>  Reserved, <b>RES0</b> .	25 {x}
[24:0 continued]	ISS	<b>13</b>  Implicit error synchronization event.  <b>0b0</b>  The SError interrupt was either not synchronized by the implicit error synchronization event or not taken immediately.  <b>0b1</b>  The SError interrupt was synchronized by the implicit error synchronization event and taken immediately.	25 {x}
[24:0 continued]	ISS	<b>12:10</b>  Asynchronous Error Type.  When DFSC is 0b010001, describes the PE error state after taking the SError interrupt exception.  <b>0b000</b> Uncontainable (UC).  <b>0b001</b> Unrecoverable state (UEU).  <b>0b010</b> Restartable state (UEO).  <b>0b011</b> Recoverable state (UER).  <b>0b110</b> Corrected (CE).	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<p><b>9</b></p> <p>External abort type. When DFSC is 0b010001, provides an IMPLEMENTATION DEFINED classification of External aborts.</p> <p>This field is valid only if the DFSC code is 0b010001. It is <b>RES0</b> for all other errors.</p> <p><b>8:6</b></p> <p>Reserved, <b>RES0</b>.</p> <p><b>5:0</b></p> <p>Data Fault Status Code.</p> <p><b>0b000000</b></p> <p>Uncategorized error.</p> <p><b>0b010001</b></p> <p>Asynchronous SError interrupt.</p>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from a Breakpoint or Vector Catch debug exception</b></p> <p><b>24:6</b></p> <p>Reserved, <b>RES0</b>.</p> <p><b>5:0</b></p> <p>Instruction Fault Status Code.</p> <p><b>0b100010</b></p> <p>Debug exception.</p> <p>For more information about generating these exceptions:</p> <ul style="list-style-type: none"> <li>For exceptions from AArch64, see <i>Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</li> </ul>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from a Software Step exception</b></p> <p><b>24</b></p> <p>Instruction syndrome valid. Indicates whether the EX bit, ISS[6], is valid, as follows:</p> <p><b>0b0</b></p> <p>EX bit is RES0.</p> <p><b>0b1</b></p> <p>EX bit is valid.</p> <p><b>23:7</b></p> <p>Reserved, <b>RES0</b>.</p>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<p><b>6</b></p> <p>Exclusive operation. If the ISV bit is set to 1, this bit indicates whether a Load-Exclusive instruction was stepped.</p> <p><b>0b0</b></p> <p>An instruction other than a Load-Exclusive instruction was stepped.</p> <p><b>0b1</b></p> <p>A Load-Exclusive instruction was stepped.</p> <p><b>5:0</b></p> <p>Instruction Fault Status Code.</p> <p><b>0b100010</b></p> <p>Debug exception.</p> <p>For more information about generating these exceptions, see <i>Software Step exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	25 {x}
[24:0 continued]	ISS	<p><b>ISS encoding for an exception from a Watchpoint exception</b></p> <p><b>24:9</b></p> <p>Reserved, <b>RES0</b>.</p> <p><b>8</b></p> <p>Cache maintenance. Indicates whether the Watchpoint exception came from a cache maintenance or address translation instruction:</p>	25 {x}
[24:0 continued]	ISS	<p><b>0b0</b></p> <p>The Watchpoint exception was not generated by the execution of one of the System instructions identified in the description of value 1.</p> <p><b>0b1</b></p> <p>The Watchpoint exception was generated by either the execution of a cache maintenance instruction or by a synchronous Watchpoint exception on the execution of an address translation instruction. The r[DC ZVA](AArch64-dc-zva), r[DC GVA](AArch64-dc-gva), and r[DC GZVA](AArch64-dc-gzva) instructions are not classified as a cache maintenance instructions, and therefore their execution cannot cause this field to be set to 1.</p>	25 {x}
[24:0 continued]	ISS	<p><b>7</b></p> <p>Reserved, <b>RES0</b>.</p>	25 {x}
[24:0 continued]	ISS	<p><b>6</b></p> <p>Write not Read. Indicates whether the Watchpoint exception was caused by an instruction writing to a memory location, or by an instruction reading from a memory location.</p> <p><b>0b0</b></p> <p>Watchpoint exception caused by an instruction reading from a memory location.</p> <p><b>0b1</b></p> <p>Watchpoint exception caused by an instruction writing to a memory location</p>	25 {x}
[24:0 continued]	ISS	<p><b>5:0</b></p> <p>Data Fault Status Code.</p> <p><b>0b100010</b></p> <p>Debug exception.</p> <p>For more information about generating these exceptions, see <i>Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	25 {x}

Bits	Name	Description	Reset
[24:0 continued]	ISS	<b>ISS encoding for an exception from execution of a Breakpoint instruction</b> <b>24:16</b> Reserved, RES0. <b>15:0</b> Set to the instruction comment field value, zero extended as necessary. For more information about generating these exceptions, see <i>Breakpoint instruction exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Pointer Authentication instruction when HCR_EL2.API == 0    SCR_EL3.API == 0</b> <b>24:0</b> Reserved, RES0. For more information about generating these exceptions, see: <ul style="list-style-type: none"> <li>AArch64-HCR_EL2.API, for exceptions from Pointer authentication instructions, using AArch64 state, trapped to EL2.</li> </ul>	25 {x}
[24:0 continued]	ISS	<b>ISS encoding for an exception from a Pointer Authentication instruction authentication failure</b> <b>24:2</b> Reserved, RES0.	25 {x}
[24:0 continued]	ISS	<b>1</b> This field indicates whether the exception is as a result of an Instruction key or a Data key. <b>0b0</b> Instruction Key. <b>0b1</b> Data Key. <b>0</b> This field indicates whether the exception is as a result of an A key or a B key. <b>0b0</b> A key. <b>0b1</b> B key	25 {x}
[24:0 continued]	ISS	The following instructions generate an exception when the Pointer Authentication Code (PAC) is incorrect: <ul style="list-style-type: none"> <li>AUTIASP, AUTIAZ, AUTIA1716.</li> <li>AUTIBSP, AUTIBZ, AUTIB1716.</li> <li>AUTIA, AUTDA, AUTIB, AUTDB.</li> <li>AUTIZA, AUTIZB, AUTDZA, AUTDZB.</li> </ul>	25 {x}
[24:0 continued]	ISS	<ul style="list-style-type: none"> <li>RETAA, RETAB.</li> <li>BRAA, BRAB, BLRAA, BLRAB.</li> <li>BRAAZ, BRABZ, BLRAAZ, BLRABZ.</li> <li>ERETAA, ERETAB.</li> <li>LDRAA, LDRAB, whether the authenticated address is written back to the base register or not.</li> </ul>	25 {x}



Access

MRS <Xt>, ESR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0010	0b000

MSR ESR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0010	0b000

Accessibility

MRS <Xt>, ESR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ESR_EL2;
```

MSR ESR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ESR_EL2 = X[t, 64];
```

A.2.2.94 PRBAR<n>\_EL2, Protection Region Base Address Register n (EL2), n = 1 - 15

Provides access to the base address for the MPU region determined by the value of 'n' and AArch64-PRSELR\_EL2.REGION as AArch64-PRSELR\_EL2.REGION<7:4>:n.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

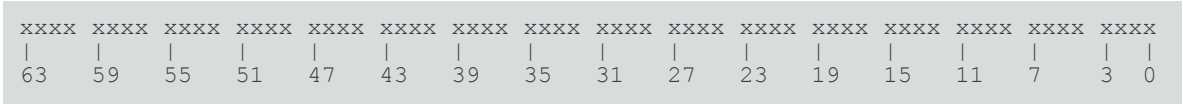
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-154: AARCH64\_PRBAR<n>\_EL2 bit assignments

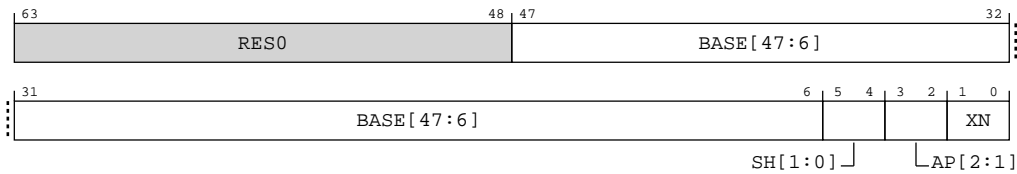


Table A-402: PRBAR<n>\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	BASE[47:6]	Bits[47:6] of the lower inclusive limit of the selected EL2 MPU memory region. This value is zero extended to provide the base address to be checked against.	42 { x }
[5:4]	SH[1:0]	Shareability attribute.  <b>0b00</b> Non-shareable  <b>0b01</b> Reserved, <b>CONSTRAINED UNPREDICTABLE</b>  <b>0b10</b> Outer Shareable  <b>0b11</b> Inner Shareable	xx
[3:2]	AP[2:1]	Access Permission attributes.  <b>0b00</b> Read/write at EL2, no access at EL1 or ELO  <b>0b01</b> Read/write at EL2, EL1 and ELO  <b>0b10</b> Read-only at EL2, no access at EL1 or ELO  <b>0b11</b> Read-only at EL2, EL1 and ELO	xx

Bits	Name	Description	Reset
[1:0]	XN	<p>Execute Never. For</p> <ul style="list-style-type: none"> <li>Stage 1 EL2 translation regime and</li> <li>Stage 2 EL1&amp;0 translation regime when FEAT_XNX is not implemented</li> </ul> <p>XN[1] determines whether execution of the instructions fetched from the MPU memory region is permitted. In this case, XN[0] is <b>RES0</b></p> <p>For stage 2 EL1&amp;0 translation regime when FEAT_XNX is implemented, the behavior of XN[1:0] is same as that defined by VMSAv8-64 for EL1&amp;0 stage 2 translation table XN[1:0].bits[54:53] field in Armv8-A architecture.</p> <p><b>0b00</b> Execution of instructions fetched from the region is permitted.</p> <p><b>0b01</b> Execution of instructions fetched from the region is not permitted.</p>	xx

### Access

Any access to MPU region register PRBAR<n>\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRBAR<n>\_EL2 return an **UNKNOWN** value.
- Writes to unimplemented PRBAR<n>\_EL2 register make all PRBAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRBAR<m>\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	'1':m[3:1]	m[0]:'00'

MSR PRBAR<m>\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	'1':m[3:1]	m[0]:'00'

### Accessibility

Any access to MPU region register PRBAR<n>\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRBAR<n>\_EL2 return an **UNKNOWN** value.
- Writes to unimplemented PRBAR<n>\_EL2 register make all PRBAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRBAR<m>\_EL2

```
integer m = UInt(CRm<2:0>:op2<2>);
```

```
if m + (UInt(PRSELR_EL2.REGION<7:4>) * 16) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRBAR_EL2[m + (UInt(AArch64-PRSELR_EL2.REGION<7:4>) * 16)];
```

MSR PRBAR<m>\_EL2, <Xt>

```
integer m = UInt(CRm<2:0>:op2<2>);
if m + (UInt(PRSELR_EL2.REGION<7:4>) * 16) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRBAR_EL2[m + (UInt(AArch64-PRSELR_EL2.REGION<7:4>) * 16)] = X[t, 64];
```

A.2.2.95 PRLAR<n>\_EL2, Protection Region Limit Address Register n (EL2), n = 1 - 15

Provides access to the limit address for the MPU region determined by the value of 'n' and AArch64-PRSELR\_EL2.REGION as AArch64-PRSELR\_EL2.REGION<7:4>:n.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

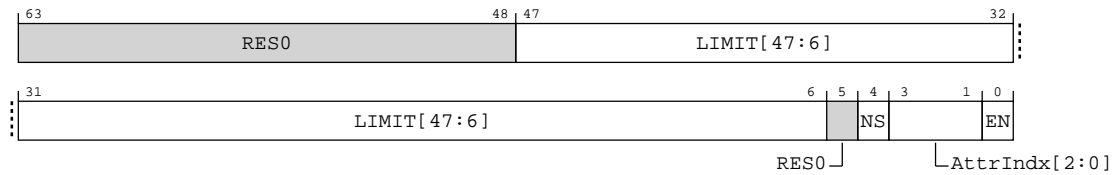
Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-155: AARCH64\_PRLAR<n>\_EL2 bit assignments****Table A-405: PRLAR<n>\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	LIMIT[47:6]	Bits[47:6] of the upper inclusive limit of the selected EL2 MPU memory region. This value is concatenated with the value 0x3F to provide the limit address to be checked against.	42 {x}
[5]	RES0	Reserved	RES0
[4]	NS	Non-secure bit. Specifies whether the output address is in the Secure or Non-secure memory.  <b>0b0</b> Output address is in Secure address space.  <b>0b1</b> Output address is in Non-secure address space.	x
[3:1]	AttrIdx[2:0]	Selects attributes from within the associated Memory Attribute Indirection Register.  <b>0b000</b> Select the Attr0 field from MAIR_EL2.  <b>0b001</b> Select the Attr1 field from MAIR_EL2.  <b>0b010</b> Select the Attr2 field from MAIR_EL2.  <b>0b011</b> Select the Attr3 field from MAIR_EL2.  <b>0b100</b> Select the Attr4 field from MAIR_EL2.  <b>0b101</b> Select the Attr5 field from MAIR_EL2.  <b>0b110</b> Select the Attr6 field from MAIR_EL2.  <b>0b111</b> Select the Attr7 field from MAIR_EL2.	xxx

Bits	Name	Description	Reset
[0]	EN	Region enable bit.  <b>0b0</b> Region disabled.  <b>0b1</b> Region enabled.	0b0

## Access

Any access to MPU region register PRLAR<n>\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRLAR<n>\_EL2 return an **UNKNOWN** value.
- Writes to unimplemented PRLAR<n>\_EL2 register make all PRLAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRLAR<m>\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	'1':m[3:1]	m[0]:'01'

MSR PRLAR<m>\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	'1':m[3:1]	m[0]:'01'

## Accessibility

Any access to MPU region register PRLAR<n>\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRLAR<n>\_EL2 return an **UNKNOWN** value.
- Writes to unimplemented PRLAR<n>\_EL2 register make all PRLAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRLAR<m>\_EL2

```
integer m = UInt(CRm<2:0>:op2<2>);
if (UInt(PRSELR_EL2.REGION<7:4>) * 16) + m >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRLAR_EL2[m + (UInt(AArch64-PRSELR_EL2.REGION<7:4>) * 16)];
```

MSR PRLAR<m>\_EL2, <Xt>

```
integer m = UInt(CRm<2:0>:op2<2>);
if (UInt(PRSELR_EL2.REGION<7:4>) * 16) + m >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRLAR_EL2[m + (UInt(AArch64-PRSELR_EL2.REGION<7:4>) * 16)] = X[t, 64];
```

A.2.2.96 FAR\_EL2, Fault Address Register (EL2)

Holds the faulting Virtual Address for all synchronous Instruction Abort exceptions, Data Abort exceptions, PC alignment fault exceptions and Watchpoint exceptions that are taken to EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-156: AARCH64\_FAR\_EL2 bit assignments

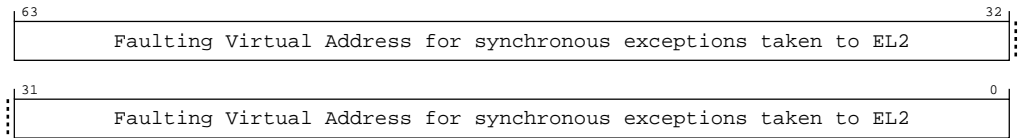


Table A-408: FAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	<p>Faulting Virtual Address for synchronous exceptions taken to EL2. Exceptions that set the FAR_EL2 are Instruction Aborts (EC 0x20 or 0x21), Data Aborts (EC 0x24 or 0x25), PC alignment faults (EC 0x22), and Watchpoints (EC 0x34 or 0x35). AArch64-ESR_EL2.EC holds the EC value for the exception.</p> <p>For a synchronous External abort, if the VA that generated the abort was from an address range for which TCR_ELx.TBI{&lt;0 1&gt;} == 1 for the translation regime in use when the abort was generated, then the top eight bits of FAR_EL2 are <b>UNKNOWN</b>.</p> <p>For a synchronous External abort other than a synchronous External abort on a translation table walk, this field is valid only if AArch64-ESR_EL2.FnV is 0, and FAR_EL2 is <b>UNKNOWN</b> if AArch64-ESR_EL2.FnV is 1.</p> <p>If a memory fault that sets FAR_EL2, other than a Tag Check Fault, is generated from a data cache maintenance or other DC instruction, this field holds the address specified in the register argument of the instruction.</p> <p>For a Data Abort exception or Watchpoint exception, if address tagging is enabled for the address accessed by the data access that caused the exception, then this field includes the tag. For more information about address tagging, see <i>Address tagging</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>Execution at EL1 or EL0 makes FAR_EL2 become <b>UNKNOWN</b>.</p> <p><b>Note:</b> The address held in this field is an address accessed by the instruction fetch or data access that caused the exception that actually gave rise to the instruction or data abort. It is the lower address that gave rise to the fault that is reported. Where different faults from different addresses arise from the same instruction, such as for an instruction that loads or stores an unaligned address that crosses a page boundary, the architecture does not prioritize which fault is reported.</p> <p>For all other exceptions taken to EL2, FAR_EL2 is <b>UNKNOWN</b>.</p> <p>FAR_EL2 is made <b>UNKNOWN</b> on an exception return from EL2.</p>	64 {x}

Access

MRS <Xt>, FAR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0000	0b000

MSR FAR\_EL2, <Xt>



op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0000	0b000

Accessibility

MRS <Xt>, FAR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = FAR_EL2;
```

MSR FAR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    FAR_EL2 = X[t, 64];
```

A.2.2.97 HPFAR\_EL2, Hypervisor IPA Fault Address Register


Holds the faulting IPA for some aborts on a stage 2 translation taken to EL2.

Configurations

The HPFAR\_EL2 is written for:

- Translation or Access faults in the second stage of translation.
- An abort in the second stage of translation performed during the translation table walk of a first stage translation, caused by a Translation fault, an Access flag fault, or a Permission fault.
- A stage 2 Address size fault.

For all other exceptions taken to EL2, this register is UNKNOWN.



Note

The address held in this register is an address accessed by the instruction fetch or data access that caused the exception that gave rise to the Instruction Abort exception or Data Abort exception. It is the lower address that gave rise to the fault that is reported. Where different faults from different addresses arise from the same instruction, such as for an instruction that loads or stores an unaligned address that crosses a page boundary, the architecture does not prioritize which fault is reported.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Execution at EL1 or EL0 makes HPFAR\_EL2 become **UNKNOWN**.

Figure A-157: AARCH64\_HPFAAR\_EL2 bit assignments

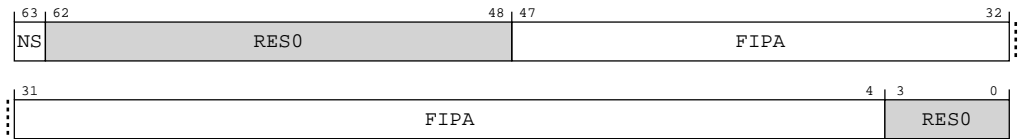


Table A-411: HPFAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63]	NS	Faulting IPA address space. <b>0b0</b> Faulting IPA is from the Secure IPA space. <b>0b1</b> Faulting IPA is from the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
47:4	FIPA	<b>FIPA encoding for None</b> <b>43:36</b> Reserved, <b>RES0</b> . <b>35:0</b> Bits[47:12] Faulting Intermediate Physical Address.  For implementations with fewer than 48 physical address bits, the corresponding upper bits in this field are <b>RES0</b> .	4 4 { x }
[3:0]	RES0	Reserved	RES0

Access

MRS <Xt>, HPFAR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0000	0b100

MSR HPFAR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0000	0b100

Accessibility

MRS <Xt>, HPFAR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = HPFAR_EL2;
```

MSR HPFAR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    HPFAR_EL2 = X[t, 64];
```

A.2.2.98 PRENR\_EL2, Protection Region Enable Register (EL2)

Provides direct access to the AArch64-PRLAR\_EL2.EN bits of EL2 MPU regions from 0 to 31.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control


Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------

6359555147433935312723191511730



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-158: AARCH64\_PRENR\_EL2 bit assignments

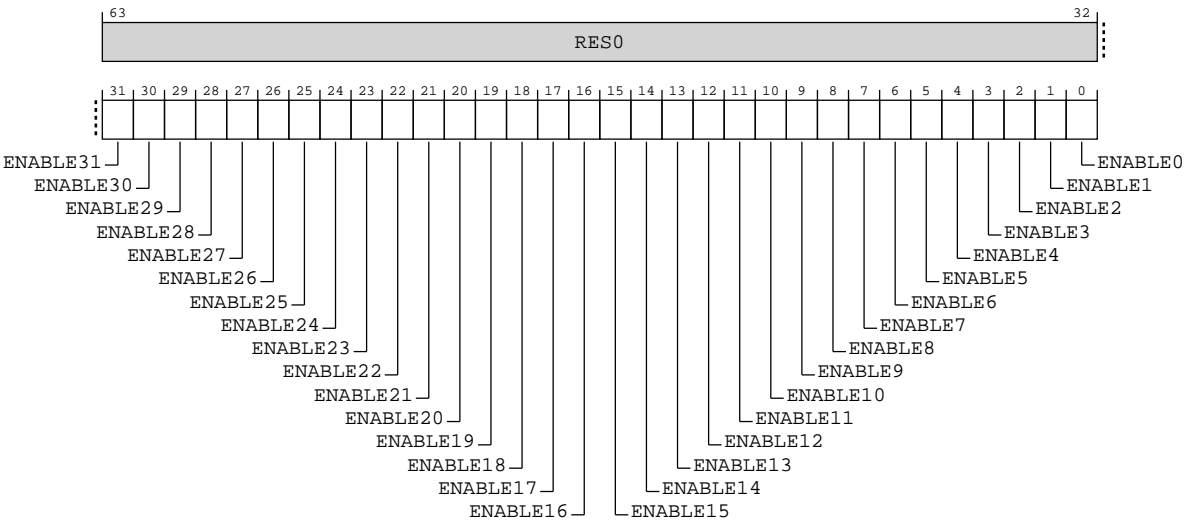


Table A-414: PRENR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	ENABLE<n>, bit[n], where n = 31 to 0	Enable bit. Each bit, n, enables or disables the respective EL2 MPU region. The bits associated with the unimplemented MPU regions are <b>RAZ/WI</b> .  0b0 Disables the EL2 MPU n region.  0b1 Enables the EL2 MPU n region.	0x00000000

Access

MRS <Xt>, PRENR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0001	0b001

MSR PRENR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0001	0b001

Accessibility

MRS <Xt>, PRENR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRENR_EL2;
```

MSR PRENR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRENR_EL2 = X[t, 64];
```

A.2.2.99 PRSELR\_EL2, Protection Region Selection Register (EL2)

Selects the region number for the EL2 MPU region associated with the AArch64-PRBAR\_EL2 and AArch64-PRLAR\_EL2 registers.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-159: AARCH64\_PRSELR\_EL2 bit assignments

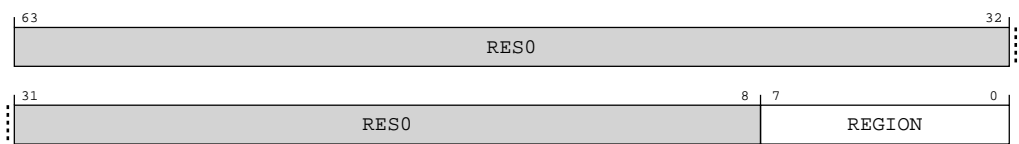


Table A-417: PRSELR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	REGION	The number of the current EL2 MPU region visible in AArch64-PRBAR_EL2 and AArch64-PRLAR_EL2. For N implemented MPU regions, memory region numbering starts at 0 and increments by 1 to the value N-1.  Writing a value greater than or equal to the number of implemented MPU regions specified by AArch64-MPUIR_EL2.REGION, results in CONSTRAINED UNPREDICTABLE behavior.  CONSTRAINED UNPREDICTABLE behavior is that PRSELR_EL2 register becomes <b>UNKNOWN</b> .	8 {x}

Access

MRS <Xt>, PRSELR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0010	0b001

MSR PRSELR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b0010	0b001

Accessibility

MRS <Xt>, PRSELR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRSELR_EL2;
```

MSR PRSELR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRSELR_EL2 = X[t, 64];
```

A.2.2.100 PRBAR\_EL2, Protection Region Base Address Register (EL2)

Provides access to the base addresses for the EL2 MPU region. AArch64-PRSELR\_EL2.REGION determines which MPU region is selected.

Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-160: AARCH64\_PRBAR\_EL2 bit assignments

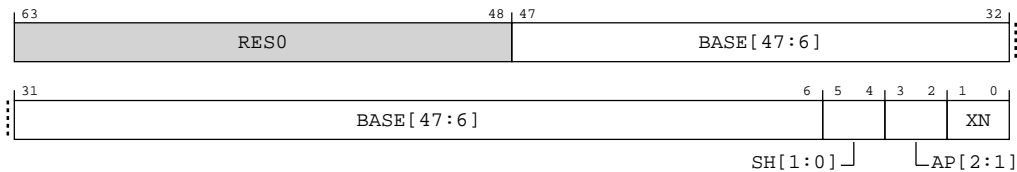


Table A-420: PRBAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	BASE[47:6]	Bits[47:6] of the lower inclusive limit of the selected EL2 MPU memory region. This value is zero extended to provide the base address to be checked against.	42 {x}

Bits	Name	Description	Reset
[5:4]	SH[1:0]	Shareability attribute.  <b>0b00</b> Non-shareable  <b>0b01</b> Reserved, <b>CONSTRAINED UNPREDICTABLE</b>  <b>0b10</b> Outer Shareable  <b>0b11</b> Inner Shareable	xx
[3:2]	AP[2:1]	Access Permission attributes.  <b>0b00</b> Read/write at EL2, no access at EL1 or EL0  <b>0b01</b> Read/write at EL2, EL1 and EL0  <b>0b10</b> Read-only at EL2, no access at EL1 or EL0  <b>0b11</b> Read-only at EL2, EL1 and EL0	xx
[1:0]	XN	Execute Never. For <ul style="list-style-type: none"> <li>Stage 1 EL2 translation regime and</li> <li>Stage 2 EL1&amp;0 translation regime when FEAT_XNX is not implemented</li> </ul> <p>XN[1] determines whether execution of the instructions fetched from the MPU memory region is permitted. In this case, XN[0] is <b>RES0</b></p> <p>For stage 2 EL1&amp;0 translation regime when FEAT_XNX is implemented, the behavior of XN[1:0] is same as that defined by VMSAv8-64 for EL1&amp;0 stage 2 translation table XN[1:0],bits[54:53] field in Armv8-A architecture.</p> <b>0b00</b> Execution of instructions fetched from the region is permitted.  <b>0b01</b> Execution of instructions fetched from the region is not permitted.	xx

## Access

Any access to MPU region register PRBAR\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRBAR\_EL2 register return an **UNKNOWN** value.
- Writes to unimplemented PRBAR\_EL2 register make all PRBAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRBAR\_EL2



op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b1000	0b000

MSR PRBAR\_EL2, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b1000	0b000

### Accessibility

Any access to MPU region register PRBAR\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRBAR\_EL2 register return an UNKNOWN value.
- Writes to unimplemented PRBAR\_EL2 register make all PRBAR\_EL2 registers value UNKNOWN.

MRS &lt;Xt&gt;, PRBAR\_EL2

```

if UInt(PRSELR_EL2.REGION) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRBAR_EL2[UInt(AArch64-PRSELR_EL2.REGION)];

```

MSR PRBAR\_EL2, &lt;Xt&gt;

```

if UInt(PRSELR_EL2.REGION) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRBAR_EL2[UInt(AArch64-PRSELR_EL2.REGION)] = X[t, 64];

```

#### A.2.2.101 PRLAR\_EL2, Protection Region Limit Address Register (EL2)

Provides access to the limit addresses for the EL2 MPU region. AArch64-PRSELR\_EL2.REGION determines which MPU region is selected.

### Configurations

All bits above implemented physical address range in this register should be treated as RES0.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-161: AARCH64\_PRLAR\_EL2 bit assignments

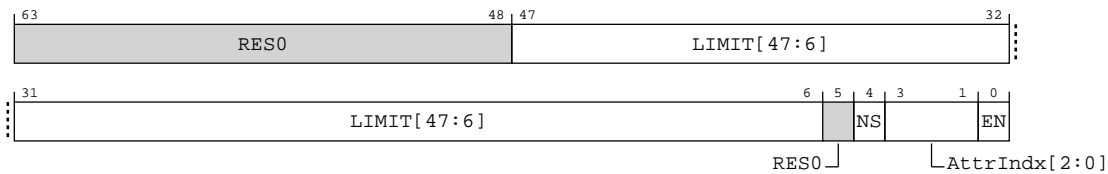


Table A-423: PRLAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:6]	LIMIT[47:6]	Bits[47:6] of the upper inclusive limit of the selected EL2 MPU memory region. This value is concatenated with the value 0x3F to provide the limit address to be checked against.	42 {x}
[5]	RES0	Reserved	RES0
[4]	NS	Non-secure bit. Specifies whether the output address is in the Secure or Non-secure memory.  <b>0b0</b> Output address is in Secure address space.  <b>0b1</b> Output address is in Non-secure address space.	x

Bits	Name	Description	Reset
[3:1]	AttrIdx[2:0]	<p>Selects attributes from within the associated Memory Attribute Indirection Register.</p> <p><b>0b000</b> Select the Attr0 field from MAIR_EL2.</p> <p><b>0b001</b> Select the Attr1 field from MAIR_EL2.</p> <p><b>0b010</b> Select the Attr2 field from MAIR_EL2.</p> <p><b>0b011</b> Select the Attr3 field from MAIR_EL2.</p> <p><b>0b100</b> Select the Attr4 field from MAIR_EL2.</p> <p><b>0b101</b> Select the Attr5 field from MAIR_EL2.</p> <p><b>0b110</b> Select the Attr6 field from MAIR_EL2.</p> <p><b>0b111</b> Select the Attr7 field from MAIR_EL2.</p>	xxx
[0]	EN	<p>Region enable bit.</p> <p><b>0b0</b> Region disabled.</p> <p><b>0b1</b> Region enabled.</p>	0b0

## Access

Any access to MPU region register PRLAR\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is **CONSTRAINED UNPREDICTABLE**.

**CONSTRAINED UNPREDICTABLE** behavior is defined as:

- Reads of unimplemented PRLAR\_EL2 register return an **UNKNOWN** value.
- Writes to unimplemented PRLAR\_EL2 register make all PRLAR\_EL2 registers value **UNKNOWN**.

MRS <Xt>, PRLAR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b1000	0b001

MSR PRLAR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0110	0b1000	0b001

## Accessibility

Any access to MPU region register PRLAR\_EL2 above the number of implemented regions specified by AArch64-MPUIR\_EL2.REGION is CONSTRAINED UNPREDICTABLE.

CONSTRAINED UNPREDICTABLE behavior is defined as:

- Reads of unimplemented PRLAR\_EL2 register return an UNKNOWN value.
- Writes to unimplemented PRLAR\_EL2 register make all PRLAR\_EL2 registers value UNKNOWN.

MRS <Xt>, PRLAR\_EL2

```

if UInt(PRSEL_R_EL2.REGION) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PRLAR_EL2[UInt(AArch64-PRSEL_R_EL2.REGION)];

```

MSR PRLAR\_EL2, <Xt>

```

if UInt(PRSEL_R_EL2.REGION) >= UInt(MPUIR_EL2.REGION) then
    ConstrainUnpredictableProcedure(Unpredictable_UnimplementedMPURegion_RW_UNKNOWN);
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    PRLAR_EL2[UInt(AArch64-PRSEL_R_EL2.REGION)] = X[t, 64];

```

### A.2.2.102 MAIR\_EL2, Memory Attribute Indirection Register (EL2)

Provides the memory attribute encodings corresponding to the possible AttrIdx values in AArch64-PRLAR\_EL2 for stage 1 EL2 translation regime and for stage 2 EL1&0 translation regime.

For stage 2 EL1&0 translations, the memory attributes are derived from MAIR\_EL2 register as described in the Armv8-R AArch64 architecture.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

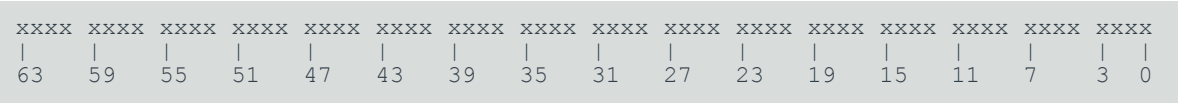
### Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

MAIR\_EL2 is permitted to be cached in a TLB.

Figure A-162: AARCH64\_MAIR\_EL2 bit assignments

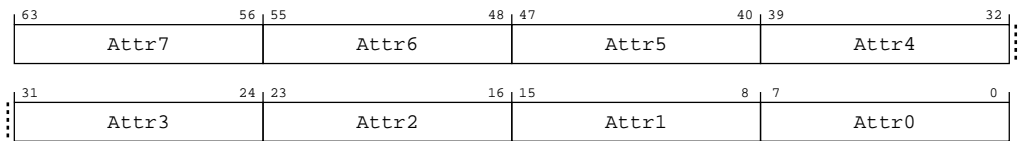


Table A-426: MAIR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	Attr<n>	The memory attribute encoding for an AttrIdx[2:0] gives the value of <n> in Attr<n>.  Attr is encoded as follows: <a href="#">Table A-427: Attr description</a> on page 737  'dd' is encoded as follows: <a href="#">Table A-428: dd description</a> on page 738  'oooo' is encoded as follows: <a href="#">Table A-429: 'oooo' description</a> on page 738  R = Outer Read-Allocate policy, W = Outer Write-Allocate policy.  'iiii' is encoded as follows: <a href="#">Table A-430: 'iiii' description</a> on page 738  R = Inner Read-Allocate policy, W = Inner Write-Allocate policy.  The R and W bits in 'oooo' and 'iiii' fields have the following meanings: <a href="#">Table A-431: R or W description</a> on page 738	64 {x}

Table A-427: Attr description

Attr	Meaning
0b0000dd00	Device memory. See encoding of 'dd' for the type of Device memory.
0b0000ddxx, (xx != 00)	UNPREDICTABLE.
0boooooiiii, (oooo != 0000 and iiii != 0000)	Normal memory. See encoding of 'oooo' and 'iiii' for the type of Normal Memory.

Attr	Meaning
0bxxxx0000, where xxxx != 0000	UNPREDICTABLE.

**Table A-428: dd description**

dd	Meaning
0b00	Device-nGnRnE memory
0b01	Device-nGnRE memory
0b10	Device-nGRE memory
0b11	Device-GRE memory

**Table A-429: 'oooo' description**

'oooo'	Meaning
0b0000	See encoding of Attr
0b00RW, RW not 0b00	Normal memory, Outer Write-Through Transient
0b0100	Normal memory, Outer Non-cacheable
0b01RW, RW not 0b00	Normal memory, Outer Write-Back Transient
0b10RW	Normal memory, Outer Write-Through Non-transient
0b11RW	Normal memory, Outer Write-Back Non-transient

**Table A-430: 'iiii' description**

'iiii'	Meaning
0b0000	See encoding of Attr
0b00RW, RW not 0b00	Normal memory, Inner Write-Through Transient
0b0100	Normal memory, Inner Non-cacheable
0b01RW, RW not 0b00	Normal memory, Inner Write-Back Transient
0b10RW	Normal memory, Inner Write-Through Non-transient
0b11RW	Normal memory, Inner Write-Back Non-transient

**Table A-431: R or W description**

R or W	Meaning
0b0	No Allocate
0b1	Allocate

## Access

MRS &lt;Xt&gt;, MAIR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1010	0b0010	0b000

MSR MAIR\_EL2, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b100	0b1010	0b0010	0b000

MRS &lt;Xt&gt;, MAIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0010	0b000

MSR MAIR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1010	0b0010	0b000

## Accessibility

MRS &lt;Xt&gt;, MAIR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MAIR_EL2;

```

MSR MAIR\_EL2, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    MAIR_EL2 = X[t, 64];

```

MRS &lt;Xt&gt;, MAIR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TRVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MAIR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MAIR_EL1;

```

MSR MAIR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TVM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        MAIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    MAIR_EL1 = X[t, 64];

```

A.2.2.103 AMAIR\_EL2, Auxiliary Memory Attribute Indirection Register (EL2)

Provides **IMPLEMENTATION DEFINED** memory attributes for the memory regions specified by AArch64-MAIR\_EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

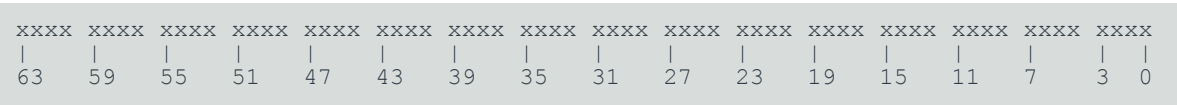
Functional group

Generic System Control

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-163: AARCH64\_AMAIR\_EL2 bit assignments

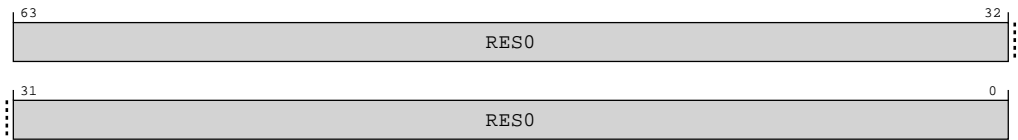


Table A-436: AMAIR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, AMAIR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1010	0b0011	0b000



MSR AMAIR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1010	0b0011	0b000

Accessibility

MRS <Xt>, AMAIR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = AMAIR_EL2;
```

MSR AMAIR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AMAIR_EL2 = X[t, 64];
```

A.2.2.104 VBAR\_EL2, Vector Base Address Register (EL2)

Holds the vector base address for any exception that is taken to EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-164: AARCH64\_VBAR\_EL2 bit assignments

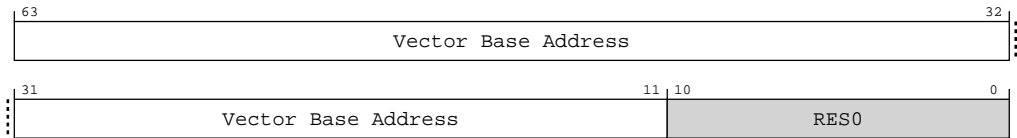


Table A-439: VBAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:11]	None	Vector Base Address. Base address of the exception vectors for exceptions taken to EL2.  <b>Note:</b> <ul style="list-style-type: none"><li>If tagged addresses are being used, bits [55:48] of VBAR_EL2 must be 0 or else the use of the vector address will result in a recursive exception.</li><li>If tagged addresses are not being used, bits [63:48] of VBAR_EL2 must be 0 or else the use of the vector address will result in a recursive exception.</li></ul>	53 {x}
[10:0]	RES0	Reserved	RES0

Access

MRS <Xt>, VBAR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0000	0b000

MSR VBAR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0000	0b000

Accessibility

MRS <Xt>, VBAR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VBAR_EL2;
```

MSR VBAR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    VBAR_EL2 = X[t, 64];
```

A.2.2.105 RVBAR\_EL2, Reset Vector Base Address Register (if EL3 not implemented)

Contains the **IMPLEMENTATION DEFINED** address that execution starts from after reset.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-165: AARCH64\_RVBAR\_EL2 bit assignments



Table A-442: RVBAR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	ResetAddress	The <b>IMPLEMENTATION DEFINED</b> address that execution starts from after reset when executing in 64-bit state. Bits[1:0] of this register are 00, as this address must be aligned, and the address must be within the physical address size supported by the PE.  This field takes the value of the CFGRVBARADDRm configuration pins.	64 {x}

Access

MRS <Xt>, RVBAR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0000	0b001

Accessibility

MRS <Xt>, RVBAR\_EL2

```
if PSTATE.EL == EL2 then
    X[t, 64] = RVBAR_EL2;
else
    UNDEFINED;
```

A.2.2.106 RMR\_EL2, Reset Management Register (EL2)

A write to the register at EL2 can request a Warm reset.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx0x
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-166: AARCH64\_RMR\_EL2 bit assignments

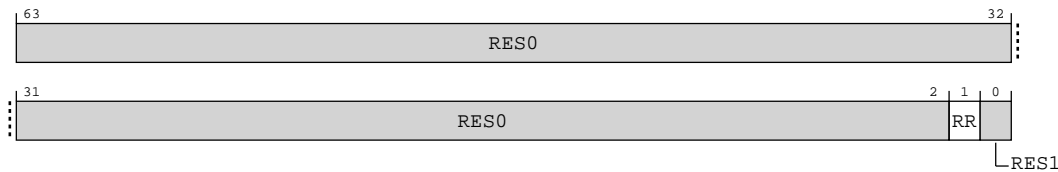


Table A-444: RMR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:2]	RES0	Reserved	RES0
[1]	RR	Reset Request. Setting this bit to 1 requests a Warm reset.  0b0 No effect.  0b1 Warm reset requested.	0b0
[0]	RES1	Reserved	RES1

Access

MRS <Xt>, RMR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0000	0b010

MSR RMR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0000	0b010

Accessibility

MRS <Xt>, RMR\_EL2

```
if PSTATE.EL == EL2 then
    X[t, 64] = RMR_EL2;
else
    UNDEFINED;
```

MSR RMR\_EL2, <Xt>

```
if PSTATE.EL == EL2 then
    RMR_EL2 = X[t, 64];
else
    UNDEFINED;
```

A.2.2.107 CONTEXTIDR\_EL2, Context ID Register (EL2)

Identifies the current Process Identifier for EL2.

The value of the whole of this register is called the Context ID and is used by:

- The debug logic, for Linked and Unlinked Context ID matching.
- The trace logic, to identify the current process.

The significance of this register is for debug and trace use only.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-167: AARCH64\_CONTEXTIDR\_EL2 bit assignments

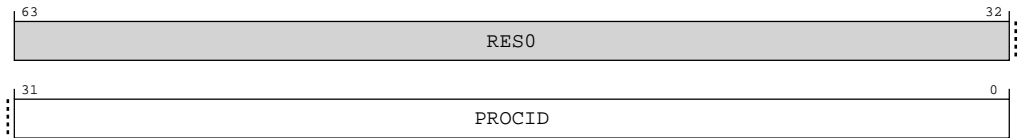


Table A-447: CONTEXTIDR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	PROCID	Process Identifier. This field must be programmed with a unique value that identifies the current process.	32 {x}

Access

MRS <Xt>, CONTEXTIDR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1101	0b0000	0b001

MSR CONTEXTIDR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1101	0b0000	0b001

Accessibility

MRS <Xt>, CONTEXTIDR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CONTEXTIDR_EL2;
```

MSR CONTEXTIDR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    CONTEXTIDR_EL2 = X[t, 64];
```

A.2.2.108 TPIDR\_EL2, EL2 Software Thread ID Register

Provides a location where software executing at EL2 can store thread identifying information, for OS management purposes.

The PE makes no use of this register.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-168: AARCH64\_TPIDR\_EL2 bit assignments

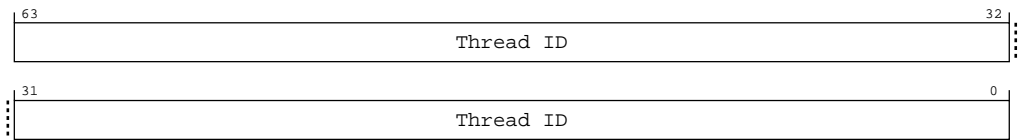


Table A-450: TPIDR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Thread ID. Thread identifying information stored by software running at this Exception level.	64 {x}

Access

MRS <Xt>, TPIDR\_EL2



op0	op1	CRn	CRm	op2
0b11	0b100	0b1101	0b0000	0b010

MSR TPIDR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1101	0b0000	0b010

Accessibility

MRS <Xt>, TPIDR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = TPIDR_EL2;
```

MSR TPIDR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    TPIDR_EL2 = X[t, 64];
```

A.2.2.109 IMP\_INTLATENCY\_EL2, Interrupt Latency Register

This register provides controls to the Hypervisor to limit certain memory transactions which could negatively impact the processor interrupt latency or the freedom from interference.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic System Control

Access type

See bit descriptions

Reset value

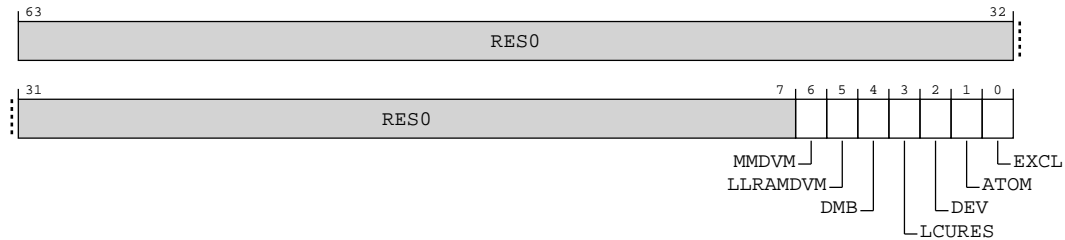
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x0x0	x000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-169: AARCH64\_IMP\_INTLATENCY\_EL2 bit assignments**



**Table A-453: IMP\_INTLATENCY\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:7]	RES0	Reserved	RES0
[6]	MMDVM	<p>Limit the behavior of instruction cache maintenance instructions to the MM port.</p> <p><b>0b0</b></p> <p>No impact on instruction cache maintenance instructions that target the MM port.</p> <p><b>0b1</b></p> <p>Causes instruction cache maintenance instructions that target the MM port to generate a Data Abort.</p> <p><b>Note:</b></p> <p>This includes IC IALLUIS and IC IALLU instructions as these always target the MM port.</p>	0b0
[5]	LLRAMDVM	<p><b>When CFGLLRAMIMP == 1</b></p> <p>Limit the behavior of instruction cache maintenance instructions to the LLRAM port.</p> <p><b>0b0</b></p> <p>No impact on instruction cache maintenance instructions that target the LLRAM port.</p> <p><b>0b1</b></p> <p>Causes instruction cache maintenance instructions that target the LLRAM port to generate a Data Abort.</p> <p><b>Otherwise</b></p> <p>RES0</p>	'0'
[4]	DMB	<p>Controls the Data Memory Barrier (DMB) instruction behavior.</p> <p><b>0b0</b></p> <p>This field has no effect on the DMB behavior.</p> <p><b>0b1</b></p> <p>Forces AArch64-IMP_CPUACTLR_EL1.DMB to behave as if it is 0b1, regardless of the actual value of this bit.</p>	0b0

Bits	Name	Description	Reset
[3]	LCURES	<p><b>When CFGLLRAMIMP == 1 or CFGSPPIMP == 1</b></p> <p>Force CPU resources reservation for LCU (LLRAM and SPP) accesses.</p> <p><b>0b0</b></p> <p>No impact on CPU resources reservation.</p> <p><b>0b1</b></p> <p>Forces AArch64-IMP_CPUACTLR_EL1.LCURES to behave as if it is 0b1, regardless of the actual value of this bit.</p> <p><b>Otherwise</b></p> <p>RESO</p>	'0'
[2]	DEV	<p>Limit Device accesses on the MM or LLRAM ports.</p> <p><b>0b0</b></p> <p>No impact on Device accesses.</p> <p><b>0b1</b></p> <p>Causes any Device access on the MM or LLRAM ports to generate a Data Abort. Also causes any access to the LLPP port which cross a 128-bit boundary or SPP port which cross a 64-bit boundary to generate a Data Abort.</p>	0b0
[1]	ATOM	<p>Limit the behavior of certain atomic accesses:</p> <ul style="list-style-type: none"> <li>All atomic accesses to the MM port.</li> <li>All non-cacheable atomic accesses to the LLRAM port.</li> <li>If CFGLLRAMSHARED == 1, all outer-shareable atomic accesses to the LLRAM port.</li> </ul> <p><b>0b0</b></p> <p>No impact on atomic accesses.</p> <p><b>0b1</b></p> <p>If attributes to the atomic accesses listed above can be changed to execute near, they are forced to do so. Otherwise, causes these far accesses to generate a Data Abort. This setting overrides any behavior selected by AArch64-IMP_CPUACTLR_EL1.ATOM.</p>	0b0
[0]	EXCL	<p>Limit the behavior of certain exclusive accesses:</p> <ul style="list-style-type: none"> <li>All non-cacheable exclusive accesses to the MM port.</li> <li>All non-cacheable exclusive accesses to the LLRAM port.</li> <li>If CFGLLRAMSHARED == 1, all outer-shareable exclusive accesses to the LLRAM port.</li> </ul> <p><b>0b0</b></p> <p>No impact on exclusive accesses.</p> <p><b>0b1</b></p> <p>Causes the exclusive accesses listed above to generate a Data Abort.</p>	0b0

## Access

MRS <Xt>, IMP\_INTLATENCY\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1111	0b0001	0b111

MSR IMP\_INTLATENCY\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1111	0b0001	0b111

## Accessibility

MRS <Xt>, IMP\_INTLATENCY\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_INTLATENCY_EL2;
```

MSR IMP\_INTLATENCY\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    IMP_INTLATENCY_EL2 = X[t, 64];
```

## A.2.3 AArch64 Performance Monitors register description

This section includes the register descriptions for all Performance Monitors registers in the Cortex®-R82AE processor.

### A.2.3.1 PMINTENSET\_EL1, Performance Monitors Interrupt Enable Set Register

Enables the generation of interrupt requests

on overflows from

the cycle counter, AArch64-PMCCNTR\_ELO, and the event counters AArch64-PMEVCNTR<n>\_ELO. Reading the register shows which overflow interrupt requests

are enabled.

## Configurations

AArch64 register PMINTENSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.8.11 PMINTENSET\\_EL1, Performance Monitors Interrupt Enable Set Register](#) on page 2228 bits [31:0].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-170: AARCH64\_PMINTENSET\_EL1 bit assignments

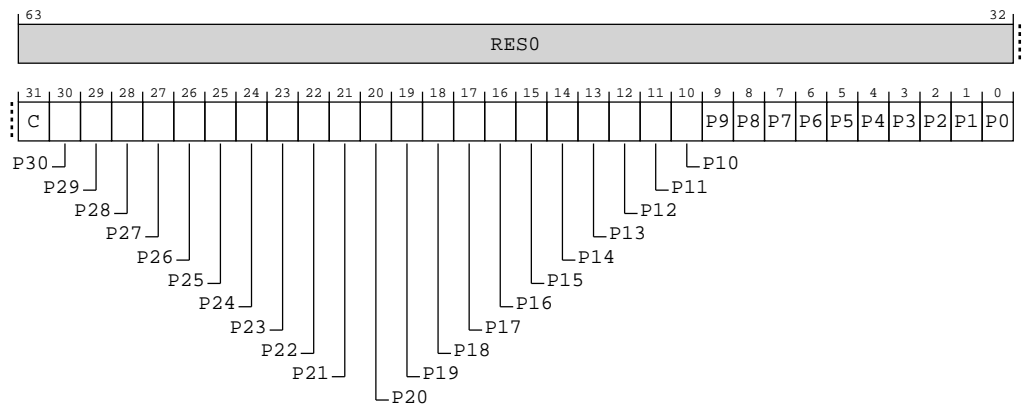


Table A-456: PMINTENSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31]	C	<p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO enable. On writes, allows software to enable the interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO. On reads, returns the interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO enabled.</p> <p>Access to this field is W1S.</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable. On writes, allows software to enable the interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO. On reads, returns the interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1S.</li> </ul>	31 {x}

## Access

MRS <Xt>, PMINTENSET\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1001	0b1110	0b001

MSR PMINTENSET\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1001	0b1110	0b001

## Accessibility

MRS <Xt>, PMINTENSET\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMINTENSET_EL1;

```

```
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMINTENSET_EL1;
```

MSR PMINTENSET\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMINTENSET_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMINTENSET_EL1 = X[t, 64];
```

A.2.3.2 PMINTENCLR\_EL1, Performance Monitors Interrupt Enable Clear Register

Disables the generation of interrupt requests  
on overflows from  
the cycle counter, AArch64-PMCCNTR\_ELO, and the event counters AArch64-  
PMEVCNTR<n>\_ELO. Reading the register shows which overflow interrupt requests  
are enabled.

Configurations

AArch64 register PMINTENCLR\_EL1 bits [31:0] are architecturally mapped to External register  
B.2.2.8.12 PMINTENCLR\_EL1, Performance Monitors Interrupt Enable Clear Register on page  
2230 bits [31:0].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-171: AARCH64\_PMINTENCLR\_EL1 bit assignments

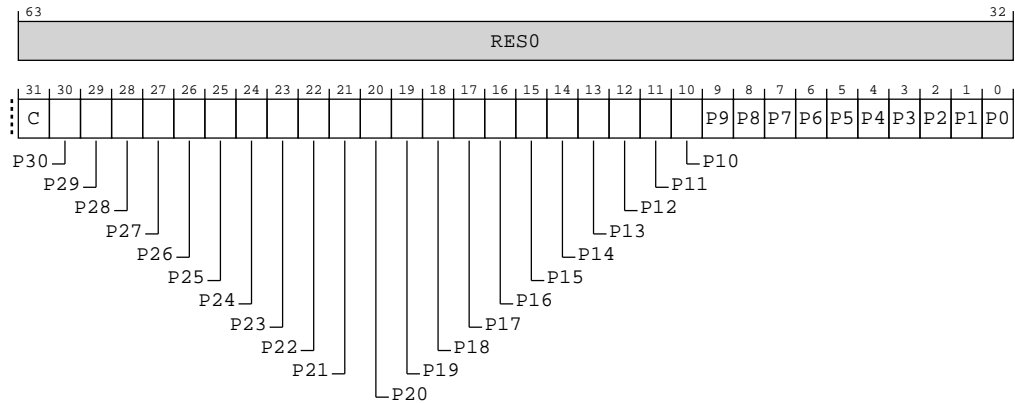


Table A-459: PMINTENCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO disable. On writes, allows software to disable the interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO. On reads, returns the interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request on unsigned overflow of AArch64-PMCCNTR_ELO enabled.</p> <p>Access to this field is W1C.</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disable. On writes, allows software to disable the interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO. On reads, returns the interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1C.</li> </ul>	31 {x}



Access

MRS <Xt>, PMINTENCLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1001	0b1110	0b010

MSR PMINTENCLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1001	0b1110	0b010

Accessibility

MRS <Xt>, PMINTENCLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMINTENCLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMINTENCLR_EL1;
```

MSR PMINTENCLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMINTENCLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMINTENCLR_EL1 = X[t, 64];
```

A.2.3.3 PMMIR\_EL1, Performance Monitors Machine Identification Register

Describes Performance Monitors parameters specific to the implementation to software.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0110	0000	0010	0000	0011
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-172: AARCH64\_PMMIR\_EL1 bit assignments

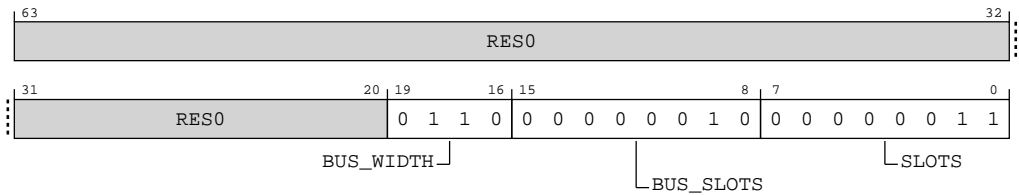


Table A-462: PMMIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0
[19:16]	BUS_WIDTH	Bus width. Indicates the number of bytes each BUS_ACCESS event relates to. Encoded as Log <sub>2</sub> (number of bytes), plus one.  <b>0b0110</b> 32 bytes.  All other values are reserved.  Each transfer is up to this number of bytes. An access might be smaller than the bus width.  When this field is nonzero, each access counted by BUS_ACCESS is at most BUS_WIDTH bytes. An implementation might treat a wide bus as multiple narrower buses, such that a wide access on the bus increments the BUS_ACCESS counter by more than one.	0b0110
[15:8]	BUS_SLOTS	Bus count. The largest value by which the BUS_ACCESS event might increment in a single BUS_CYCLES cycle.  <b>0b00000010</b> The BUS_ACCESS event might increment by at most 2 in a single BUS_CYCLES cycle.  When this field is nonzero, the largest value by which the BUS_ACCESS event might increment in a single BUS_CYCLES cycle is BUS_SLOTS.  If the bus count information is not available, this field will read as zero.	0x02

Bits	Name	Description	Reset
[7:0]	SLOTS	Operation width. The largest value by which the STALL_SLOT event might increment in a single cycle.  <b>0b00000011</b> STALL_SLOT may increment by up to 3 in a single cycle.	0x03

### Access

MRS &lt;Xt&gt;, PMMIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1001	0b1110	0b110

### Accessibility

MRS &lt;Xt&gt;, PMMIR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMMIR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMMIR_EL1;

```

## A.2.3.4 IMP\_CLUSTERPMCR\_EL1, Cluster Performance Monitors Control Register

Provides details of the cluster Performance Monitors implementation, including the number of counters implemented, and configures and controls the counters.

### Configurations

AArch64 register IMP\_CLUSTERPMCR\_EL1 bits [7:0] are architecturally mapped to External register [B.2.2.2.13 CLUSTERPMU\\_PMCR\\_EL1, Cluster Performance Monitors Control Register](#) on page 1823 bits [7:0].

### Attributes

#### Width

64

#### Functional group

Performance Monitors registers

#### Access type

RO

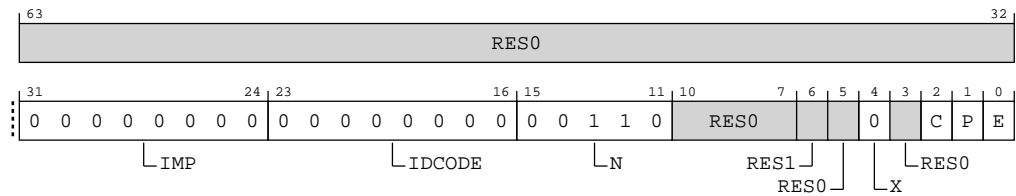
#### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0011	0xxx	xxx0	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-173: AARCH64\_IMP\_CLUSTERPMCR\_EL1 bit assignments****Table A-464: IMP\_CLUSTERPMCR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:24]	IMP	Implementer code.  <b>0b00000000</b> No ID information is present.  Access to this field is: RO	0x00
[23:16]	IDCODE	Identification code.  <b>0b00000000</b> No ID information is present.  Access to this field is: RO	0x00
[15:11]	N	Indicates the number of event counters implemented.  <b>0b00110</b> 6 counters implemented.  Access to this field is: RO	0b00110
[10:7]	RES0	Reserved	RES0
[6]	RES1	Reserved	RES1
[5]	RES0	Reserved	RES0
[4]	X	This field enables the exporting of events over an event bus to another device.  <b>0b0</b> Cluster PMU events are not exported externally.  Access to this field is: RO	0b0
[3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2]	C	<p>Cycle counter reset. This bit is WO. The effects of writing to this bit are:</p> <p><b>0b0</b> No action.</p> <p><b>0b1</b> Reset AArch64-IMP_CLUSTERPMCCNTR_EL1 to zero.</p> <p>This bit is always <b>RAZ</b>.</p> <p><b>Note:</b> Resetting AArch64-IMP_CLUSTERPMCCNTR_EL1 does not change the cycle counter overflow bit.</p>	x
[1]	P	<p>Event counter reset. This bit is WO. The effects of writing to this bit are:</p> <p><b>0b0</b> No action.</p> <p><b>0b1</b> Reset all event counters, not including AArch64-IMP_CLUSTERPMCCNTR_EL1, to zero.</p> <p>This bit is always <b>RAZ</b>.</p> <p>A write of 1 to this bit resets all the event counters.</p> <p>Resetting the event counters does not change the event counter overflow bits.</p>	x
[0]	E	<p>Enable.</p> <p><b>0b0</b> All event counters, including AArch64-IMP_CLUSTERPMCCNTR_EL1, are disabled.</p> <p><b>0b1</b> All event counters can be enabled by AArch64-IMP_CLUSTERPMCCNTENSET_EL1.</p> <p>This bit is RW.</p>	0b0

## Access

MRS <Xt>, IMP\_CLUSTERPMCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b000

MSR IMP\_CLUSTERPMCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b000

## Accessibility

MRS <Xt>, IMP\_CLUSTERPMCR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then

```

```
if HCR_EL2.TIDCP == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = IMP_CLUSTERPMCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCR_EL1;
```

MSR IMP\_CLUSTERPMCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMCR_EL1 = X[t, 64];
```

### A.2.3.5 IMP\_CLUSTERPMCNTENSET\_EL1, Cluster Performance Monitors Count Enable Set register

Enables the Cluster Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and any implemented event counters. Reading this register shows which counters are enabled.

#### Configurations

AArch64 register IMP\_CLUSTERPMCNTENSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.5 CLUSTERPMU\\_PMCNTENSET\\_EL1, Cluster Performance Monitors Count Enable Set register](#) on page 1810 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-174: AARCH64\_IMP\_CLUSTERPMCNTENSET\_EL1 bit assignments

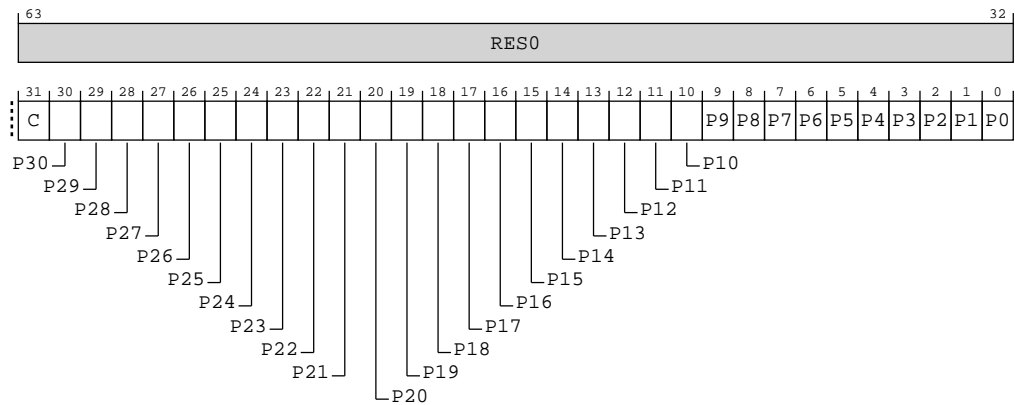


Table A-467: IMP\_CLUSTERPMCNTENSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	AArch64-IMP_CLUSTERPMCCNTR_EL1 enable bit. Enables the cycle counter register. Possible values are:  <b>0b0</b> When read, means the cycle counter is disabled. When written, has no effect.  <b>0b1</b> When read, means the cycle counter is enabled. When written, enables the cycle counter.	x
[30:0]	P<n>, bit[n], where n = 30 to 0	Event counter enable bit for ext-CLUSTERPMU_PMEVCNTR<n>_EL1.  Bits [30:6] are <b>RAZ/WI</b> .  <b>0b0</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is disabled. When written, has no effect.  <b>0b1</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 event counter is enabled. When written, enables ext-CLUSTERPMU_PMEVCNTR<n>_EL1.	31 {x}

## Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCNTENSET\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b001

MSR IMP\_CLUSTERPMCNTENSET\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b001

## Accessibility

MRS <Xt>, IMP\_CLUSTERPMCNTENSET\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCNTENSET_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERPMCNTENSET_EL1;

```

MSR IMP\_CLUSTERPMCNTENSET\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCNTENSET_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_CLUSTERPMCNTENSET_EL1 = X[t, 64];

```

### A.2.3.6 IMP\_CLUSTERPMCNTENCLR\_EL1, Cluster Performance Monitors Count Enable Clear register

Disables the Cluster Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and any implemented event counters. Reading this register shows which counters are enabled.

#### Configurations

AArch64 register IMP\_CLUSTERPMCNTENCLR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.6 CLUSTERPMU\\_PMCNTENCLR\\_EL1, Cluster Performance Monitors Count Enable Clear register](#) on page 1812 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

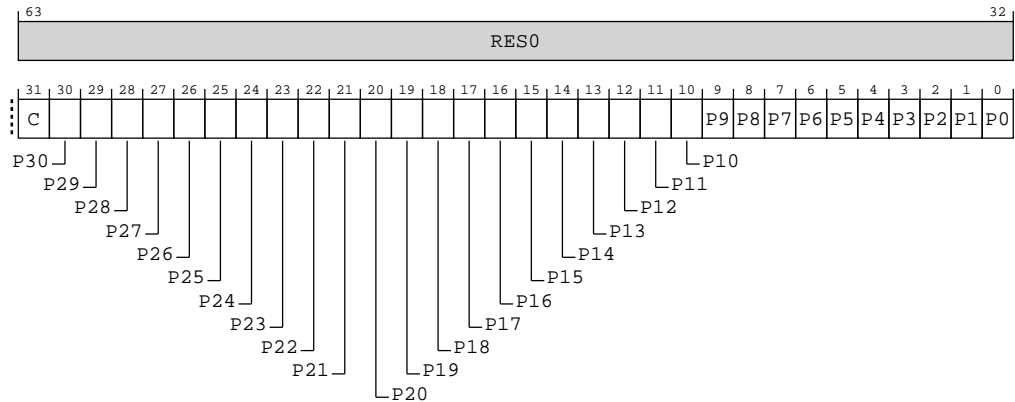
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-175: AARCH64\_IMP\_CLUSTERPMCNTENCLR\_EL1 bit assignments****Table A-470: IMP\_CLUSTERPMCNTENCLR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	AArch64-IMP_CLUSTERPMCNTENCLR_EL1 disable bit. Disables the cycle counter register. Possible values are:  <b>0b0</b> When read, means the cycle counter is disabled. When written, has no effect.  <b>0b1</b> When read, means the cycle counter is enabled. When written, disables the cycle counter.	x
[30:0]	P<n>, bit[n], where n = 30 to 0	Event counter disable bit for ext-CLUSTERPMU_PMEVCNTR<n>_EL1.  Bits [30:6] are <b>RAZ/WI</b> .  <b>0b0</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is disabled. When written, has no effect.  <b>0b1</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is enabled. When written, disables ext-CLUSTERPMU_PMEVCNTR<n>_EL1.	31 {x}

## Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCNTENCLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b010

MSR IMP\_CLUSTERPMCNTENCLR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b010

**Accessibility**

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCNTENCLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCNTENCLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCNTENCLR_EL1;

```

MSR IMP\_CLUSTERPMCNTENCLR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCNTENCLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMCNTENCLR_EL1 = X[t, 64];

```

**A.2.3.7 IMP\_CLUSTERPMOVSET\_EL1, Cluster Performance Monitors Overflow Flag Status Set register**

Sets the state of the overflow bit for the Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and each of the implemented event counters.

**Configurations**

AArch64 register IMP\_CLUSTERPMOVSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.11 CLUSTERPMU\\_PMOVSET\\_EL1, Cluster Performance Monitors Overflow Flag Status Set register](#) on page 1820 bits [31:0].

**Attributes****Width**

64

**Functional group**

Performance Monitors registers

**Access type**

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-176: AARCH64\_IMP\_CLUSTERPMOVSSET\_EL1 bit assignments

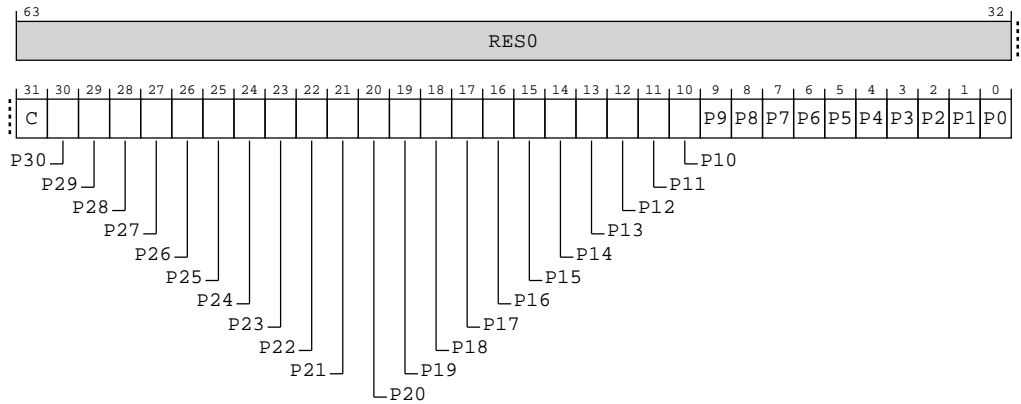


Table A-473: IMP\_CLUSTERPMOVSSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<div>Cycle counter overflow set bit.</div> <div><b>0b0</b> When read, means the cycle counter has not overflowed since this bit was last cleared. When written, has no effect.</div> <div><b>0b1</b> When read, means the cycle counter has overflowed since this bit was last cleared. When written, sets the cycle counter overflow bit to 1.</div> <div>Access to this field is W1C.</div>	x

Bits	Name	Description	Reset
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow set bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>Bits [30:6] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has overflowed since this bit was last cleared. When written, sets the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 overflow bit to 1.</p>	31 {x}

### Access

MRS <Xt>, IMP\_CLUSTERPMOVSSET\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b011

MSR IMP\_CLUSTERPMOVSSET\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b011

### Accessibility

MRS <Xt>, IMP\_CLUSTERPMOVSSET\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMOVSSET_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMOVSSET_EL1;

```

MSR IMP\_CLUSTERPMOVSSET\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMOVSSET_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMOVSSET_EL1 = X[t, 64];

```

### A.2.3.8 IMP\_CLUSTERPMOVSLR\_EL1, Cluster Performance Monitors Overflow Flag Status Clear Register

Contains the state of the overflow bit for the Cluster Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and each of the implemented event counters. Writing to this register clears these bits.

#### Configurations

AArch64 register IMP\_CLUSTERPMOVSLR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.9 CLUSTERPMU\\_PMOVSLR\\_EL1, Cluster Performance Monitors Overflow Flag Status Clear register](#) on page 1817 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

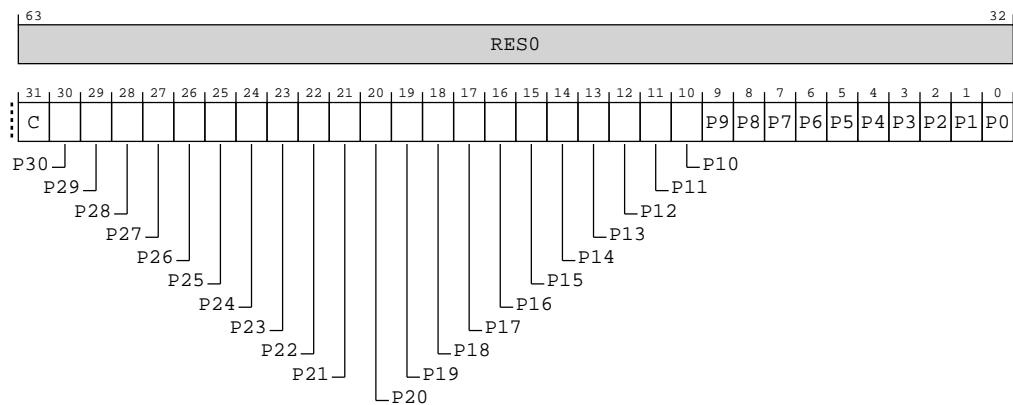


Note

Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-177: AARCH64\_IMP\_CLUSTERPMOVSLR\_EL1 bit assignments



**Table A-476: IMP\_CLUSTERPMOVSLR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>Cycle counter overflow clear bit.</p> <p><b>0b0</b></p> <p>When read, means the cycle counter has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter has overflowed since this bit was last cleared. When written, clears the cycle counter overflow bit to 0.</p> <p>Access to this field is W1C.</p>	x
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow clear bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>Bits [30:6] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has overflowed since this bit was last cleared. When written, clears the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 overflow bit to 0.</p>	31 {x}

### Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMOVSLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b100

MSR IMP\_CLUSTERPMOVSLR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b100

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERPMOVSLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMOVSLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMOVSLR_EL1;

```

MSR IMP\_CLUSTERPMOVSLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMOVSLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMOVSLR_EL1 = X[t, 64];
```

A.2.3.9 IMP\_CLUSTERPMSELR\_EL1, Cluster Performance Monitors Event Counter Selection Register

Selects the current event counter ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1 or the cycle counter, CCNT.

IMP\_CLUSTERPMSELR\_EL1 is used in conjunction with AArch64-IMP\_CLUSTERPMXEVTYPER\_EL1 to determine the event that increments a selected event counter, and the modes and states in which the selected counter increments.

It is also used in conjunction with AArch64-IMP\_CLUSTERPMXEVCNTR\_EL1, to determine the value of a selected event counter.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-178: AARCH64\_IMP\_CLUSTERPMSELR\_EL1 bit assignments

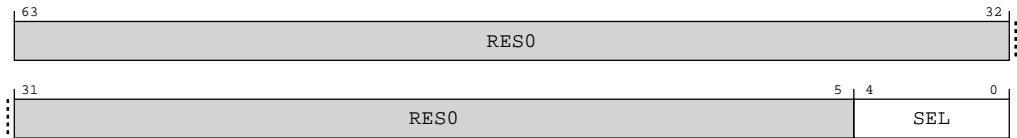


Table A-479: IMP\_CLUSTERPMSELR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:5]	RES0	Reserved	RES0
[4:0]	SEL	<p>Selects event counter, ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1, where n is the value held in this field. This value identifies which event counter is accessed when a subsequent access to AArch64-IMP_CLUSTERPMXEVTYPER_EL1 or AArch64-IMP_CLUSTERPMXEVCNTR_EL1 occurs.</p> <p>This field can take any value from 0 (0b00000) to (PMCR.N)-1, or 31 (0b11111).</p> <p>When IMP_CLUSTERPMSELR_EL1.SEL is 0b11111, it selects the cycle counter and:</p> <ul style="list-style-type: none"><li>A read of the AArch64-IMP_CLUSTERPMXEVTYPER_EL1 returns the value of AArch64-IMP_CLUSTERPMCCFILTR_EL1.</li><li>A write of the AArch64-IMP_CLUSTERPMXEVTYPER_EL1 writes to AArch64-IMP_CLUSTERPMCCFILTR_EL1.</li><li>A read or write of AArch64-IMP_CLUSTERPMXEVCNTR_EL1 has CONSTRAINED UNPREDICTABLE effects. See AArch64-IMP_CLUSTERPMXEVCNTR_EL1 for more details.</li></ul> <p>If this field is set to a value greater than or equal to the number of counters accessible at the current Exception level, but not equal to 31:</p> <ul style="list-style-type: none"><li>Direct reads of this field return an <b>UNKNOWN</b> value.</li><li>The results of access to AArch64-IMP_CLUSTERPMXEVTYPER_EL1 or AArch64-IMP_CLUSTERPMXEVCNTR_EL1 are CONSTRAINED UNPREDICTABLE. See AArch64-IMP_CLUSTERPMXEVTYPER_EL1 or AArch64-IMP_CLUSTERPMXEVCNTR_EL1 for more details.</li></ul>	5 {x}

Access

MRS <Xt>, IMP\_CLUSTERPMSELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b101

MSR IMP\_CLUSTERPMSELR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b101

Accessibility

MRS <Xt>, IMP\_CLUSTERPMSELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```



```

elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMSELR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMSELR_EL1;

```

MSR IMP\_CLUSTERPMSELR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMSELR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMSELR_EL1 = X[t, 64];

```

### A.2.3.10 IMP\_CLUSTERPMINTENSET\_EL1, Cluster Performance Monitors Interrupt Enable Set register

Enables the generation of interrupt requests on overflows from the Cluster Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and the event counters ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1. Reading the register shows which overflow interrupt requests are enabled.

#### Configurations

AArch64 register IMP\_CLUSTERPMINTENSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.7 CLUSTERPMU\\_PMINTENSET\\_EL1, Cluster Performance Monitors Interrupt Enable Set register](#) on page 1813 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

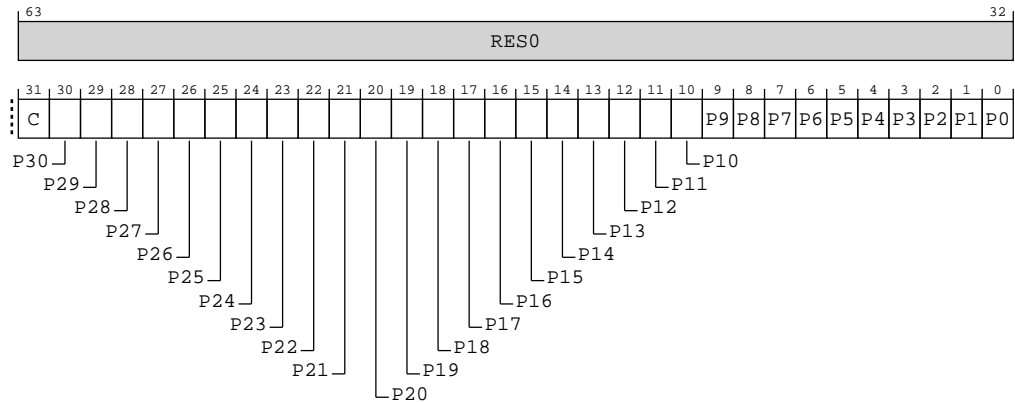
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-179: AARCH64\_IMP\_CLUSTERPMINTENSET\_EL1 bit assignments**



**Table A-482: IMP\_CLUSTERPMINTENSET\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>AArch64-IMP_CLUSTERPMCCNTR_EL1 overflow interrupt request enable bit. Possible values are:</p> <p><b>0b0</b></p> <p>When read, means the cycle counter overflow interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter overflow interrupt request is enabled. When written, enables the cycle count overflow interrupt request.</p>	x
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow interrupt request enable bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>Bits [30:6] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is enabled. When written, enables the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 interrupt request.</p>	31 {x}

## Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMINTENSET\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b110

MSR IMP\_CLUSTERPMINTENSET\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b110

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERPMINTENSET\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMINTENSET_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_CLUSTERPMINTENSET_EL1;

```

MSR IMP\_CLUSTERPMINTENSET\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMINTENSET_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_CLUSTERPMINTENSET_EL1 = X[t, 64];

```

### A.2.3.11 IMP\_CLUSTERPMINTENCLR\_EL1, Cluster Performance Monitors Interrupt Enable Clear register

Disables the generation of interrupt requests on overflows from the Cluster Cycle Count Register, AArch64-IMP\_CLUSTERPMCCNTR\_EL1, and the event counters ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1. Reading the register shows which overflow interrupt requests are enabled.

### Configurations

AArch64 register IMP\_CLUSTERPMINTENCLR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.8 CLUSTERPMU\\_PMINTENCLR\\_EL1, Cluster Performance Monitors Interrupt Enable Clear register](#) on page 1815 bits [31:0].

### Attributes

#### Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-180: AARCH64\_IMP\_CLUSTERPMINTENCLR\_EL1 bit assignments

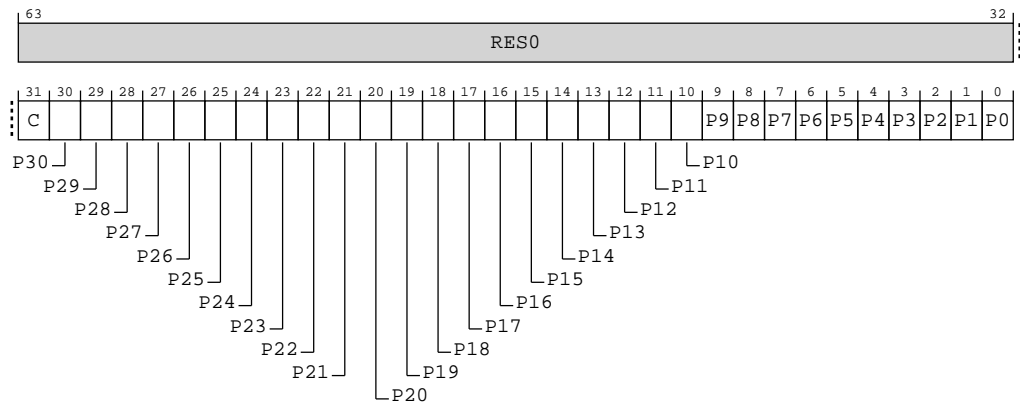


Table A-485: IMP\_CLUSTERPMINTENCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>AArch64-IMP_CLUSTERPMCCNTR_EL1 overflow interrupt request disable bit. Possible values are:</p> <p><b>0b0</b></p> <p>When read, means the cycle counter overflow interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter overflow interrupt request is enabled. When written, disables the cycle count overflow interrupt request.</p>	x

Bits	Name	Description	Reset
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow interrupt request disable bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>Bits [30:6] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is enabled. When written, disables the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 interrupt request.</p>	31 {x}

### Access

MRS <Xt>, IMP\_CLUSTERPMINTENCLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b111

MSR IMP\_CLUSTERPMINTENCLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0101	0b111

### Accessibility

MRS <Xt>, IMP\_CLUSTERPMINTENCLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMINTENCLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMINTENCLR_EL1;

```

MSR IMP\_CLUSTERPMINTENCLR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMINTENCLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMINTENCLR_EL1 = X[t, 64];

```

### A.2.3.12 IMP\_CLUSTERPMCCNTR\_EL1, Cluster Performance Monitors Cycle Count Register

Holds the value of the processor Cycle Counter, CCNT, that counts processor clock cycles. See 'Time as measured by the Performance Monitors cycle counter' in the Arm® Architecture Reference Manual, Armv8, for Armv8-A architecture profile for more information.

AArch64-IMP\_CLUSTERPMCCFILTR\_EL1 determines the modes and states in which the IMP\_CLUSTERPMCCNTR\_EL1 can increment.

#### Configurations

All counters are subject to any changes in clock frequency, including clock stopping caused by the WFI and WFE instructions. This means that it is CONSTRAINED UNPREDICTABLE whether or not IMP\_CLUSTERPMCCNTR\_EL1 continues to increment when clocks are stopped by WFI and WFE instructions.

AArch64 register IMP\_CLUSTERPMCCNTR\_EL1 bits [63:0] are architecturally mapped to External register [B.2.2.2.2 CLUSTERPMU\\_PMCCNTR\\_EL1, Cluster Performance Monitors Cycle Counter](#) on page 1805 bits [63:0].

#### Attributes

**Width**

64

**Functional group**

Performance Monitors registers

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-181: AARCH64\_IMP\_CLUSTERPMCCNTR\_EL1 bit assignments

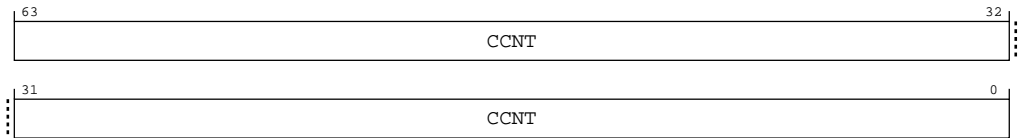


Table A-488: IMP\_CLUSTERPMCCNTR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	CCNT	Cycle count. The cycle count increments in every processor clock cycle.  Writing 1 to AArch64-IMP_CLUSTERPMCR_EL1.C sets this field to 0.	64 {x}

Access

MRS <Xt>, IMP\_CLUSTERPMCCNTR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b000

MSR IMP\_CLUSTERPMCCNTR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b000

Accessibility

MRS <Xt>, IMP\_CLUSTERPMCCNTR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCCNTR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCCNTR_EL1;
```

MSR IMP\_CLUSTERPMCCNTR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCCNTR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMCCNTR_EL1 = X[t, 64];
```

### A.2.3.13 IMP\_CLUSTERPMXEVTYPER\_EL1, Cluster Performance Monitors Selected Event Type Register

When AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL selects an event counter, this accesses a ext-CLUSTERPMU\_PMEVTYPER<n>\_EL1 register. When AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL selects the cycle counter, this accesses ext-CLUSTERPMU\_PMCCFILTR\_EL1.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

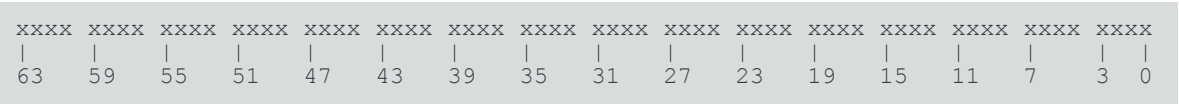
##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value



Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-182: AARCH64\_IMP\_CLUSTERPMXEVTYPER\_EL1 bit assignments

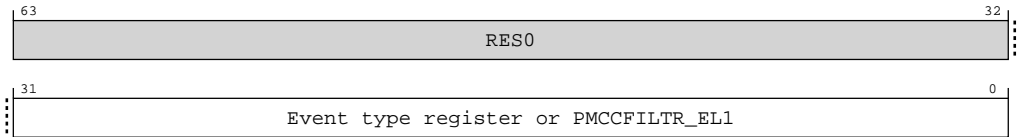


Table A-491: IMP\_CLUSTERPMXEVTYPER\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[31:0]	None	When AArch64-IMP_CLUSTERPMSELR_EL1.SEL == 31, this register accesses ext-CLUSTERPMU_PMCCFILTR_EL1.  Otherwise, this register accesses ext-CLUSTERPMU_PMEVTYPER<n>_EL1 where n is the value in AArch64-IMP_CLUSTERPMSELR_EL1.SEL.	32 {x}

### Access

If AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL is greater than or equal to the number of accessible counters then reads and writes of IMP\_CLUSTERPMXEVTYPER\_EL1 behave as if AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL has an **UNKNOWN** value less than the number of counters accessible at the current Exception level and Security state.

MRS <Xt>, IMP\_CLUSTERPMXEVTYPER\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b001

MSR IMP\_CLUSTERPMXEVTYPER\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b001

### Accessibility

If AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL is greater than or equal to the number of accessible counters then reads and writes of IMP\_CLUSTERPMXEVTYPER\_EL1 behave as if AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL has an UNKNOWN value less than the number of counters accessible at the current Exception level and Security state.

MRS <Xt>, IMP\_CLUSTERPMXEVTYPER\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMXEVTYPER_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMXEVTYPER_EL1;

```

MSR IMP\_CLUSTERPMXEVTYPER\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMXEVTYPER_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMXEVTYPER_EL1 = X[t, 64];

```

A.2.3.14 IMP\_CLUSTERPMXVCNTR\_EL1, Cluster Performance Monitors Selected Event Count Register

Reads or writes the value of the selected event counter, ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1. AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL determines which event counter is selected.

Configurations

This register is available in all configurations.

Attributes

Width

64

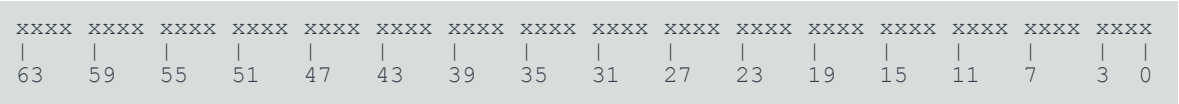
Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-183: AARCH64\_IMP\_CLUSTERPMXVCNTR\_EL1 bit assignments

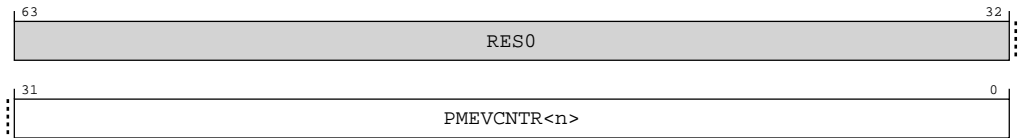


Table A-494: IMP\_CLUSTERPMXVCNTR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	PMEVCNTR<n>	Value of the selected event counter, ext-CLUSTERPMU_PMEVCNTR<n>_EL1, where n is the value stored in AArch64-IMP_CLUSTERPMSELR_EL1.SEL.	32 {x}

## Access

If AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL is greater than or equal to the number of accessible counters then reads and writes of IMP\_CLUSTERPMXVCNTR\_EL1 behave as if AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL has an **UNKNOWN** value less than the number of counters accessible at the current Exception level and Security state.

MRS <Xt>, IMP\_CLUSTERPMXVCNTR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b010

MSR IMP\_CLUSTERPMXVCNTR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b010

## Accessibility

If AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL is greater than or equal to the number of accessible counters then reads and writes of IMP\_CLUSTERPMXVCNTR\_EL1 behave as if AArch64-IMP\_CLUSTERPMSELR\_EL1.SEL has an UNKNOWN value less than the number of counters accessible at the current Exception level and Security state.

MRS <Xt>, IMP\_CLUSTERPMXVCNTR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMXVCNTR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMXVCNTR_EL1;

```

MSR IMP\_CLUSTERPMXVCNTR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMXVCNTR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_CLUSTERPMXVCNTR_EL1 = X[t, 64];

```

### A.2.3.15 IMP\_CLUSTERPMCEID0\_EL1, Cluster Performance Monitors Common Event Identification register 0

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the ranges 0x0000 to 0x001F and 0x4000 to 0x401F.

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

#### Configurations

AArch64 register IMP\_CLUSTERPMCEID0\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.14 CLUSTERPMU\\_PMCEID0, Cluster Performance Monitors Common Event Identification register 0](#) on page 1826 bits [31:0].

AArch64 register IMP\_CLUSTERPMCEID0\_EL1 bits [63:32] are architecturally mapped to External register [B.2.2.2.16 CLUSTERPMU\\_PMCEID2, Cluster Performance Monitors Common Event Identification register 2](#) on page 1833 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

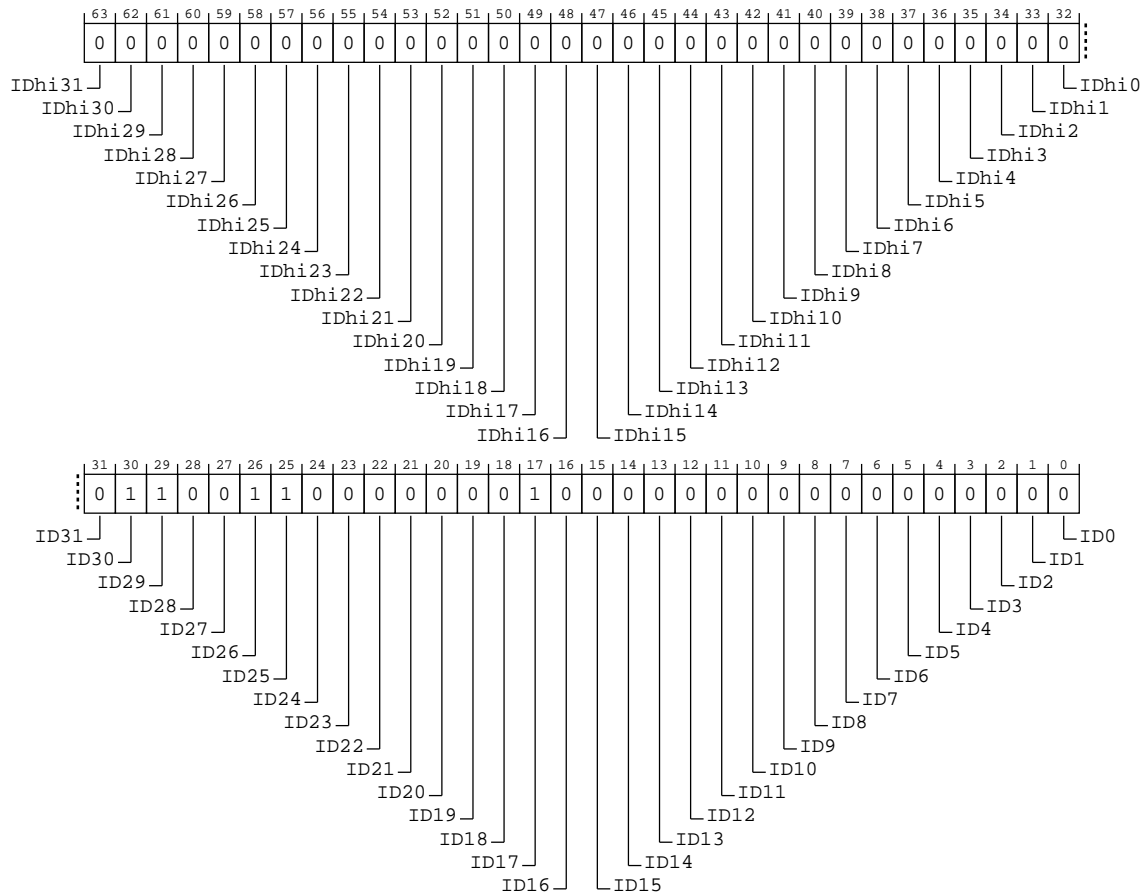
See bit descriptions

##### Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0110 0110 0000 0010 0000 0000 0000 0000

## Bit descriptions

**Figure A-184: AARCH64\_IMP\_CLUSTERPMCEID0\_EL1 bit assignments**



**Table A-497: IMP\_CLUSTERPMCEID0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63]	IDHi31	Common event 0x401F implemented. <b>0b0</b> Event 0x401F not implemented.	0b0
[62]	IDHi30	Common event 0x401E implemented. <b>0b0</b> Event 0x401E not implemented.	0b0
[61]	IDHi29	Common event 0x401D implemented. <b>0b0</b> Event 0x401D not implemented.	0b0
[60]	IDHi28	Common event 0x401C implemented. <b>0b0</b> Event 0x401C not implemented.	0b0

Bits	Name	Description	Reset
[59]	IDHi27	Common event 0x401B implemented. <b>0b0</b> Event 0x401B not implemented.	0b0
[58]	IDHi26	Common event 0x401A implemented. <b>0b0</b> Event 0x401A not implemented.	0b0
[57]	IDHi25	Common event 0x4019 implemented. <b>0b0</b> Event 0x4019 not implemented.	0b0
[56]	IDHi24	Common event 0x4018 implemented. <b>0b0</b> Event 0x4018 not implemented.	0b0
[55]	IDHi23	Common event 0x4017 implemented. <b>0b0</b> Event 0x4017 not implemented.	0b0
[54]	IDHi22	Common event 0x4016 implemented. <b>0b0</b> Event 0x4016 not implemented.	0b0
[53]	IDHi21	Common event 0x4015 implemented. <b>0b0</b> Event 0x4015 not implemented.	0b0
[52]	IDHi20	Common event 0x4014 implemented. <b>0b0</b> Event 0x4014 not implemented.	0b0
[51]	IDHi19	Common event 0x4013 implemented. <b>0b0</b> Event 0x4013 not implemented.	0b0
[50]	IDHi18	Common event 0x4012 implemented. <b>0b0</b> Event 0x4012 not implemented.	0b0
[49]	IDHi17	Common event 0x4011 implemented. <b>0b0</b> Event 0x4011 not implemented.	0b0
[48]	IDHi16	Common event 0x4010 implemented. <b>0b0</b> Event 0x4010 not implemented.	0b0
[47]	IDHi15	Common event 0x400F implemented. <b>0b0</b> Event 0x400F not implemented.	0b0
[46]	IDHi14	Common event 0x400E implemented. <b>0b0</b> Event 0x400E not implemented.	0b0

Bits	Name	Description	Reset
[45]	IDHi13	Common event 0x400D implemented. <b>0b0</b> Event 0x400D not implemented.	0b0
[44]	IDHi12	Common event 0x400C implemented. <b>0b0</b> Event 0x400C not implemented.	0b0
[43]	IDHi11	Common event 0x400B implemented. <b>0b0</b> Event 0x400B not implemented.	0b0
[42]	IDHi10	Common event 0x400A implemented. <b>0b0</b> Event 0x400A not implemented.	0b0
[41]	IDHi9	Common event 0x4009 implemented. <b>0b0</b> Event 0x4009 not implemented.	0b0
[40]	IDHi8	Common event 0x4008 implemented. <b>0b0</b> Event 0x4008 not implemented.	0b0
[39]	IDHi7	Common event 0x4007 implemented. <b>0b0</b> Event 0x4007 not implemented.	0b0
[38]	IDHi6	Common event 0x4006 implemented. <b>0b0</b> Event 0x4006 not implemented.	0b0
[37]	IDHi5	Common event 0x4005 implemented. <b>0b0</b> Event 0x4005 not implemented.	0b0
[36]	IDHi4	Common event 0x4004 implemented. <b>0b0</b> Event 0x4004 not implemented.	0b0
[35]	IDHi3	Common event 0x4003 implemented. <b>0b0</b> Event 0x4003 not implemented.	0b0
[34]	IDHi2	Common event 0x4002 implemented. <b>0b0</b> Event 0x4002 not implemented.	0b0
[33]	IDHi1	Common event 0x4001 implemented. <b>0b0</b> Event 0x4001 not implemented.	0b0
[32]	IDHi0	Common event 0x4000 implemented. <b>0b0</b> Event 0x4000 not implemented.	0b0

Bits	Name	Description	Reset
[31]	ID31	Common event 0x001F implemented. <b>0b0</b> Event 0x001F not implemented.	0b0
[30]	ID30	Common event 0x001E implemented. <b>0b1</b> CHAIN event implemented.	0b1
[29]	ID29	Common event 0x001D implemented. <b>0b1</b> BUS_CYCLES event implemented.	0b1
[28]	ID28	Common event 0x001C implemented. <b>0b0</b> Event 0x001C not implemented.	0b0
[27]	ID27	Common event 0x001B implemented. <b>0b0</b> Event 0x001B not implemented.	0b0
[26]	ID26	Common event 0x001A implemented. <b>0b1</b> MEMORY_ERROR event implemented.	0b1
[25]	ID25	Common event 0x0019 implemented. <b>0b1</b> BUS_ACCESS event implemented.	0b1
[24]	ID24	Common event 0x0018 implemented. <b>0b0</b> Event 0x0018 not implemented.	0b0
[23]	ID23	Common event 0x0017 implemented. <b>0b0</b> Event 0x0017 not implemented.	0b0
[22]	ID22	Common event 0x0016 implemented. <b>0b0</b> Event 0x0016 not implemented.	0b0
[21]	ID21	Common event 0x0015 implemented. <b>0b0</b> Event 0x0015 not implemented.	0b0
[20]	ID20	Common event 0x0014 implemented. <b>0b0</b> Event 0x0014 not implemented.	0b0
[19]	ID19	Common event 0x0013 implemented. <b>0b0</b> Event 0x0013 not implemented.	0b0
[18]	ID18	Common event 0x0012 implemented. <b>0b0</b> Event 0x0012 not implemented.	0b0



Bits	Name	Description	Reset
[17]	ID17	Common event 0x0011 implemented. <b>0b1</b> CYCLES event implemented.	0b1
[16]	ID16	Common event 0x0010 implemented. <b>0b0</b> Event 0x0010 not implemented.	0b0
[15]	ID15	Common event 0x000F implemented. <b>0b0</b> Event 0x000F not implemented.	0b0
[14]	ID14	Common event 0x000E implemented. <b>0b0</b> Event 0x000E not implemented.	0b0
[13]	ID13	Common event 0x000D implemented. <b>0b0</b> Event 0x000D not implemented.	0b0
[12]	ID12	Common event 0x000C implemented. <b>0b0</b> Event 0x000C not implemented.	0b0
[11]	ID11	Common event 0x000B implemented. <b>0b0</b> Event 0x000B not implemented.	0b0
[10]	ID10	Common event 0x000A implemented. <b>0b0</b> Event 0x000A not implemented.	0b0
[9]	ID9	Common event 0x0009 implemented. <b>0b0</b> Event 0x0009 not implemented.	0b0
[8]	ID8	Common event 0x0008 implemented. <b>0b0</b> Event 0x0008 not implemented.	0b0
[7]	ID7	Common event 0x0007 implemented. <b>0b0</b> Event 0x0007 not implemented.	0b0
[6]	ID6	Common event 0x0006 implemented. <b>0b0</b> Event 0x0006 not implemented.	0b0
[5]	ID5	Common event 0x0005 implemented. <b>0b0</b> Event 0x0005 not implemented.	0b0
[4]	ID4	Common event 0x0004 implemented. <b>0b0</b> Event 0x0004 not implemented.	0b0

Bits	Name	Description	Reset
[3]	ID3	Common event 0x0003 implemented. <b>0b0</b> Event 0x0003 not implemented.	0b0
[2]	ID2	Common event 0x0002 implemented. <b>0b0</b> Event 0x0002 not implemented.	0b0
[1]	ID1	Common event 0x0001 implemented. <b>0b0</b> Event 0x0001 not implemented.	0b0
[0]	ID0	Common event 0x0000 implemented. <b>0b0</b> Event 0x0000 not implemented.	0b0

### Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCEID0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b100

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCEID0\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCEID0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCEID0_EL1;

```

#### A.2.3.16 IMP\_CLUSTERPMCEID1\_EL1, Cluster Performance Monitors Common Event Identification register 1

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the ranges 0x0000 to 0x001F and 0x4000 to 0x401F.

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

## Configurations

AArch64 register IMP\_CLUSTERPMCEID1\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.15 CLUSTERPMU\\_PMCEID1, Cluster Performance Monitors Common Event Identification register 1](#) on page 1829 bits [31:0].

AArch64 register IMP\_CLUSTERPMCEID1\_EL1 bits [63:32] are architecturally mapped to External register [B.2.2.2.17 CLUSTERPMU\\_PMCEID3, Cluster Performance Monitors Common Event Identification register 3](#) on page 1837 bits [31:0].

## Attributes

### Width

64

### Functional group

Performance Monitors registers

### Access type

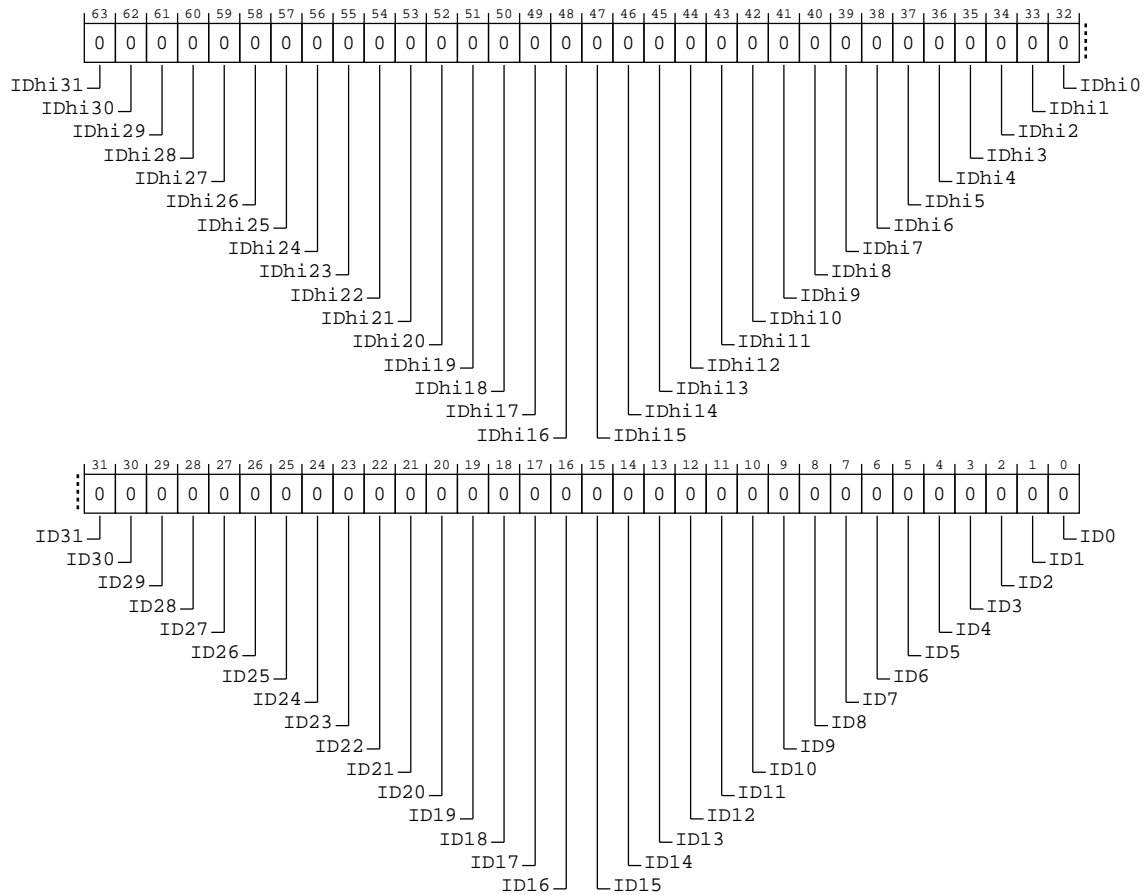
See bit descriptions

### Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

## Bit descriptions

**Figure A-185: AARCH64\_IMP\_CLUSTERPMCEID1\_EL1 bit assignments**



**Table A-499: IMP\_CLUSTERPMCEID1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63]	IDHi31	Common event 0x403F implemented. <b>0b0</b> Event 0x403F not implemented.	0b0
[62]	IDHi30	Common event 0x403E implemented. <b>0b0</b> Event 0x403E not implemented.	0b0
[61]	IDHi29	Common event 0x403D implemented. <b>0b0</b> Event 0x403D not implemented.	0b0
[60]	IDHi28	Common event 0x403C implemented. <b>0b0</b> Event 0x403C not implemented.	0b0

Bits	Name	Description	Reset
[59]	IDHi27	Common event 0x403B implemented. <b>0b0</b> Event 0x403B not implemented.	0b0
[58]	IDHi26	Common event 0x403A implemented. <b>0b0</b> Event 0x403A not implemented.	0b0
[57]	IDHi25	Common event 0x4039 implemented. <b>0b0</b> Event 0x4039 not implemented.	0b0
[56]	IDHi24	Common event 0x4038 implemented. <b>0b0</b> Event 0x4038 not implemented.	0b0
[55]	IDHi23	Common event 0x4037 implemented. <b>0b0</b> Event 0x4037 not implemented.	0b0
[54]	IDHi22	Common event 0x4036 implemented. <b>0b0</b> Event 0x4036 not implemented.	0b0
[53]	IDHi21	Common event 0x4035 implemented. <b>0b0</b> Event 0x4035 not implemented.	0b0
[52]	IDHi20	Common event 0x4034 implemented. <b>0b0</b> Event 0x4034 not implemented.	0b0
[51]	IDHi19	Common event 0x4033 implemented. <b>0b0</b> Event 0x4033 not implemented.	0b0
[50]	IDHi18	Common event 0x4032 implemented. <b>0b0</b> Event 0x4032 not implemented.	0b0
[49]	IDHi17	Common event 0x4031 implemented. <b>0b0</b> Event 0x4031 not implemented.	0b0
[48]	IDHi16	Common event 0x4030 implemented. <b>0b0</b> Event 0x4030 not implemented.	0b0
[47]	IDHi15	Common event 0x402F implemented. <b>0b0</b> Event 0x402F not implemented.	0b0
[46]	IDHi14	Common event 0x402E implemented. <b>0b0</b> Event 0x402E not implemented.	0b0

Bits	Name	Description	Reset
[45]	IDhi13	Common event 0x402D implemented. <b>0b0</b> Event 0x402D not implemented.	0b0
[44]	IDhi12	Common event 0x402C implemented. <b>0b0</b> Event 0x402C not implemented.	0b0
[43]	IDhi11	Common event 0x402B implemented. <b>0b0</b> Event 0x402B not implemented.	0b0
[42]	IDhi10	Common event 0x402A implemented. <b>0b0</b> Event 0x402A not implemented.	0b0
[41]	IDhi9	Common event 0x4029 implemented. <b>0b0</b> Event 0x4029 not implemented.	0b0
[40]	IDhi8	Common event 0x4028 implemented. <b>0b0</b> Event 0x4028 not implemented.	0b0
[39]	IDhi7	Common event 0x4027 implemented. <b>0b0</b> Event 0x4027 not implemented.	0b0
[38]	IDhi6	Common event 0x4026 implemented. <b>0b0</b> Event 0x4026 not implemented.	0b0
[37]	IDhi5	Common event 0x4025 implemented. <b>0b0</b> Event 0x4025 not implemented.	0b0
[36]	IDhi4	Common event 0x4024 implemented. <b>0b0</b> Event 0x4024 not implemented.	0b0
[35]	IDhi3	Common event 0x4023 implemented. <b>0b0</b> Event 0x4023 not implemented.	0b0
[34]	IDhi2	Common event 0x4022 implemented. <b>0b0</b> Event 0x4022 not implemented.	0b0
[33]	IDhi1	Common event 0x4021 implemented. <b>0b0</b> Event 0x4021 not implemented.	0b0
[32]	IDhi0	Common event 0x4020 implemented. <b>0b0</b> Event 0x4020 not implemented.	0b0

Bits	Name	Description	Reset
[31]	ID31	Common event 0x003F implemented. <b>0b0</b> Event 0x003F not implemented.	0b0
[30]	ID30	Common event 0x003E implemented. <b>0b0</b> Event 0x003E not implemented.	0b0
[29]	ID29	Common event 0x003D implemented. <b>0b0</b> Event 0x003D not implemented.	0b0
[28]	ID28	Common event 0x003C implemented. <b>0b0</b> Event 0x003C not implemented.	0b0
[27]	ID27	Common event 0x003B implemented. <b>0b0</b> Event 0x003B not implemented.	0b0
[26]	ID26	Common event 0x003A implemented. <b>0b0</b> Event 0x003A not implemented.	0b0
[25]	ID25	Common event 0x0039 implemented. <b>0b0</b> Event 0x0039 not implemented.	0b0
[24]	ID24	Common event 0x0038 implemented. <b>0b0</b> Event 0x0038 not implemented.	0b0
[23]	ID23	Common event 0x0037 implemented. <b>0b0</b> Event 0x0037 not implemented.	0b0
[22]	ID22	Common event 0x0036 implemented. <b>0b0</b> Event 0x0036 not implemented.	0b0
[21]	ID21	Common event 0x0035 implemented. <b>0b0</b> Event 0x0035 not implemented.	0b0
[20]	ID20	Common event 0x0034 implemented. <b>0b0</b> Event 0x0034 not implemented.	0b0
[19]	ID19	Common event 0x0033 implemented. <b>0b0</b> Event 0x0033 not implemented.	0b0
[18]	ID18	Common event 0x0032 implemented. <b>0b0</b> Event 0x0032 not implemented.	0b0

Bits	Name	Description	Reset
[17]	ID17	Common event 0x0031 implemented. <b>0b0</b> Event 0x0031 not implemented.	0b0
[16]	ID16	Common event 0x0030 implemented. <b>0b0</b> Event 0x0030 not implemented.	0b0
[15]	ID15	Common event 0x002F implemented. <b>0b0</b> Event 0x002F not implemented.	0b0
[14]	ID14	Common event 0x002E implemented. <b>0b0</b> Event 0x002E not implemented.	0b0
[13]	ID13	Common event 0x002D implemented. <b>0b0</b> Event 0x002D not implemented.	0b0
[12]	ID12	Common event 0x002C implemented. <b>0b0</b> Event 0x002C not implemented.	0b0
[11]	ID11	Common event 0x002B implemented. <b>0b0</b> Event 0x002B not implemented.	0b0
[10]	ID10	Common event 0x002A implemented. <b>0b0</b> Event 0x002A not implemented.	0b0
[9]	ID9	Common event 0x0029 implemented. <b>0b0</b> Event 0x0029 not implemented.	0b0
[8]	ID8	Common event 0x0028 implemented. <b>0b0</b> Event 0x0028 not implemented.	0b0
[7]	ID7	Common event 0x0027 implemented. <b>0b0</b> Event 0x0027 not implemented.	0b0
[6]	ID6	Common event 0x0026 implemented. <b>0b0</b> Event 0x0026 not implemented.	0b0
[5]	ID5	Common event 0x0025 implemented. <b>0b0</b> Event 0x0025 not implemented.	0b0
[4]	ID4	Common event 0x0024 implemented. <b>0b0</b> Event 0x0024 not implemented.	0b0



Bits	Name	Description	Reset
[3]	ID3	Common event 0x0023 implemented. <b>0b0</b> Event 0x0023 not implemented.	0b0
[2]	ID2	Common event 0x0022 implemented. <b>0b0</b> Event 0x0022 not implemented.	0b0
[1]	ID1	Common event 0x0021 implemented. <b>0b0</b> Event 0x0021 not implemented.	0b0
[0]	ID0	Common event 0x0020 implemented. <b>0b0</b> Event 0x0020 not implemented.	0b0

### Access

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCEID1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b101

### Accessibility

MRS &lt;Xt&gt;, IMP\_CLUSTERPMCEID1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCEID1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCEID1_EL1;

```

## A.2.3.17 IMP\_CLUSTERPMCLAIMSET\_EL1, Cluster Performance Monitors Claim Set register

Used by software to set CLAIM bits to 1.

### Configurations

AArch64 register IMP\_CLUSTERPMCLAIMSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.20 CLUSTERPMU\\_PMCLAIMSET\\_EL1, Cluster Performance Monitors Claim Set register](#) on page 1843 bits [31:0].

### Attributes

#### Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-186: AARCH64\_IMP\_CLUSTERPMCLAIMSET\_EL1 bit assignments

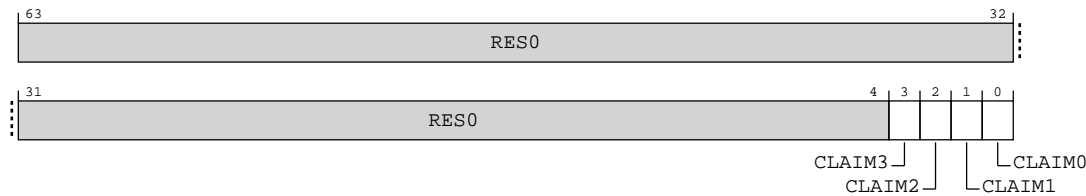


Table A-501: IMP\_CLUSTERPMCLAIMSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	CLAIM tag set bit.  <b>0b0</b> No action.  <b>0b1</b> Indirectly set claim bit to 1.	xxxxx <sup>19</sup>

Access

MRS <Xt>, IMP\_CLUSTERPMCLAIMSET\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b110

MSR IMP\_CLUSTERPMCLAIMSET\_EL1, <Xt>

<sup>19</sup> An External Debug reset clears the CLAIM tag bits to 0.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.  
Non-Confidential

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b110

## Accessibility

MRS <Xt>, IMP\_CLUSTERPMCLAIMSET\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_CLUSTERPMCLAIMSET_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCLAIMSET_EL1;
```

MSR IMP\_CLUSTERPMCLAIMSET\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCLAIMSET_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_CLUSTERPMCLAIMSET_EL1 = X[t, 64];
```

## A.2.3.18 IMP\_CLUSTERPMCLAIMCLR\_EL1, Cluster Performance Monitors Claim Clear register

Used by software to read the values of the CLAIM bits, and to clear these bits to 0.

### Configurations

AArch64 register IMP\_CLUSTERPMCLAIMCLR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.2.21 CLUSTERPMU\\_PMCLAIMCLR\\_EL1, Cluster Performance Monitors Claim Clear register](#) on page 1844 bits [31:0].

### Attributes

#### Width

64

#### Functional group

Performance Monitors registers


#### Access type

See bit descriptions

#### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------

6359555147433935312723191511730



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-187: AARCH64\_IMP\_CLUSTERPMCLAIMCLR\_EL1 bit assignments

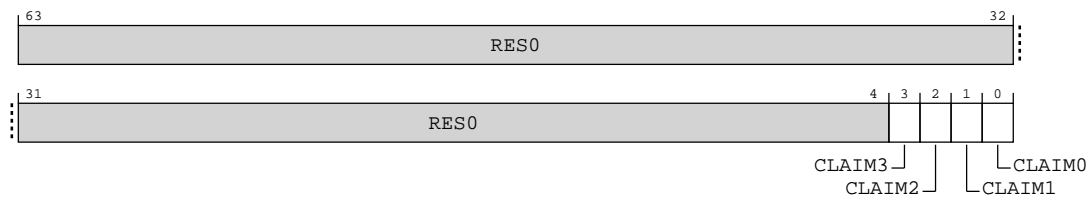


Table A-504: IMP\_CLUSTERPMCLAIMCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	CLAIM tag clear bit.  <b>0b0</b> No action.  <b>0b1</b> Indirectly clear claim bit to 0.	xxxx <sup>20</sup>

Access

MRS <Xt>, IMP\_CLUSTERPMCLAIMCLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b111

MSR IMP\_CLUSTERPMCLAIMCLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0110	0b111

Accessibility

MRS <Xt>, IMP\_CLUSTERPMCLAIMCLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
```

<sup>20</sup> An External Debug reset clears the CLAIM tag bits to 0.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.  
Non-Confidential

Page 800 of 2314

```
if HCR_EL2.TIDCP == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    X[t, 64] = IMP_CLUSTERPMCLAIMCLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_CLUSTERPMCLAIMCLR_EL1;
```

MSR IMP\_CLUSTERPMCLAIMCLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CLPMU == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_CLUSTERPMCLAIMCLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_CLUSTERPMCLAIMCLR_EL1 = X[t, 64];
```

A.2.3.19 PMCR\_ELO, Performance Monitors Control Register

Provides details of the Performance Monitors implementation, including the number of counters implemented, and configures and controls the counters.

Configurations

AArch64 register PMCR\_ELO bits [63:32, 10:0] are architecturally mapped to External register [B.2.2.8.17 PMCR\\_ELO, Performance Monitors Control Register](#) on page 2240 bits [63:32].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

RAZW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0011	0xxx	xxx0	x000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-188: AARCH64\_PMCR\_ELO bit assignments

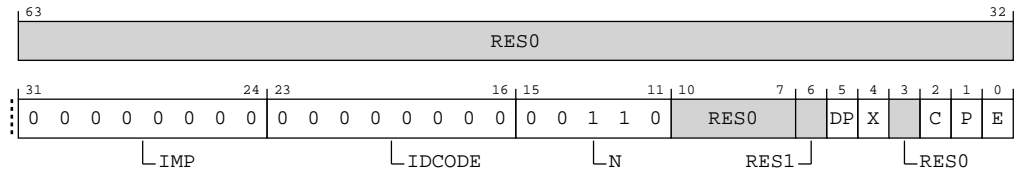


Table A-507: PMCR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:24]	IMP	Implementer code. PMCR_ELO.IDCODE is <b>RES0</b> and software must use AArch64-MIDR_EL1 to identify the PE.  <b>0b00000000</b> No ID information is present.  Use of this field is deprecated.	0x00
[23:16]	IDCODE	Identification code.  <b>0b00000000</b> No ID information is present.	0x00
[15:11]	N	Indicates the number of event counters implemented. Reads of this field from EL1 and EL0 return the value of AArch64-MDCR_EL2.HPMN.  <b>0b00110</b> 6 counters implemented.	0b00110
[10:7]	RES0	Reserved	RES0
[6]	RES1	Reserved	RES1
[5]	DP	Disable cycle counter when event counting is prohibited.  <b>0b0</b> Cycle counting by AArch64-PMCCNTR_ELO is not affected by this mechanism.  <b>0b1</b> Cycle counting by AArch64-PMCCNTR_ELO is disabled in prohibited regions and when event counting is frozen: <ul style="list-style-type: none"> <li>If FEAT_PMUv3p1 is implemented, EL2 is implemented, and AArch64-MDCR_EL2.HPMD is 1, then cycle counting by AArch64-PMCCNTR_ELO is disabled at EL2.</li> </ul> <p>The conditions when this field disables the cycle counter are the same as when event counting by an event counter AArch64-PMEVCNTR&lt;n&gt;_ELO is prohibited or frozen, when either EL2 is not implemented or n is less than AArch64-MDCR_EL2.HPMN.</p> <p>For more information, see <i>Prohibiting event and cycle counting</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x

Bits	Name	Description	Reset
[4]	X	<p>Enable export of events to the core trace unit (ETM).</p> <p><b>0b0</b></p> <p>Do not export events.</p> <p><b>0b1</b></p> <p>Export events to the ETM, where not prohibited.</p>	0b0
[3]	RES0	Reserved	RES0
[2]	C	<p>Cycle counter reset. The effects of writing to this bit are:</p> <p><b>0b0</b></p> <p>No action.</p> <p><b>0b1</b></p> <p>Reset AArch64-PMCCNTR_ELO to zero.</p> <p>Resetting AArch64-PMCCNTR_ELO does not change the cycle counter overflow bit.</p> <p>Access to this field is: WO/<b>RAZ</b></p>	0b0
[1]	P	<p>Event counter reset.</p> <p>In the description of this field, PMN is PMCR_ELO.N.</p> <p><b>0b0</b></p> <p>No action.</p> <p><b>0b1</b></p> <p>If n is in the range of affected event counters, resets each event counter AArch64-PMEVCNTR&lt;n&gt;_ELO to zero.</p> <p>The effects of writing to this bit are:</p> <ul style="list-style-type: none"> <li>• If EL2 is implemented and enabled in the current Security state, in EL0 and EL1, if PMN is not 0, a write of 1 to this bit resets event counters in the range [0 .. (PMN-1)].</li> <li>• In EL2, a write of 1 to this bit resets all the event counters.</li> <li>• This field does not affect the operation of other event counters and AArch64-PMCCNTR_ELO.</li> </ul> <p>Resetting the event counters does not change the event counter overflow bits.</p> <p>Access to this field is: WO/<b>RAZ</b></p>	0b0

Bits	Name	Description	Reset
[0]	E	<p>Enable.</p> <p>In the description of this field:</p> <ul style="list-style-type: none"> <li>If EL2 is implemented, then PMN is AArch64-MDCR_EL2.HPMN.</li> <li>If EL2 is not implemented, then PMN is PMCR_ELO.N.</li> </ul> <p><b>0b0</b></p> <p>Affected counters are disabled and do not count.</p> <p><b>0b1</b></p> <p>Affected counters are enabled by AArch64-PMCNTENSET_ELO.</p> <p>The counters affected by this field are:</p> <ul style="list-style-type: none"> <li>If EL2 is implemented, event counters AArch64-PMEVCNTR&lt;n&gt;_ELO for values of n less than PMN. This applies even when EL2 is disabled in the current Security state.</li> <li>If EL2 is not implemented, all event counters AArch64-PMEVCNTR&lt;n&gt;_ELO.</li> <li>The cycle counter AArch64-PMCCNTR_ELO.</li> </ul> <p>Other event counters are not affected by this field.</p>	0b0

## Access

MRS <Xt>, PMCR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b000

MSR PMCR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b000

## Accessibility

MRS <Xt>, PMCR\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elsif MDCR_EL2.TPMCR == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCR_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elsif MDCR_EL2.TPMCR == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCR_ELO;

```



```
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMCR_EL0;
```

### MSR PMCR\_EL0, <Xt>

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif MDCR_EL2.TPMCR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMCR_EL0 = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif MDCR_EL2.TPMCR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMCR_EL0 = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMCR_EL0 = X[t, 64];
```

### A.2.3.20 PMCNTENSET\_EL0, Performance Monitors Count Enable Set Register

Enables the Cycle Count Register, AArch64-PMCCNTR\_EL0, and any implemented event counters AArch64-PMEVCNTR<n>\_EL0. Reading this register shows which counters are enabled.

#### Configurations

AArch64 register PMCNTENSET\_EL0 bits [31:0] are architecturally mapped to External register [B.2.2.8.9 PMCNTENSET\\_EL0, Performance Monitors Count Enable Set Register](#) on page 2225 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-189: AARCH64\_PMCNTENSET\_ELO bit assignments

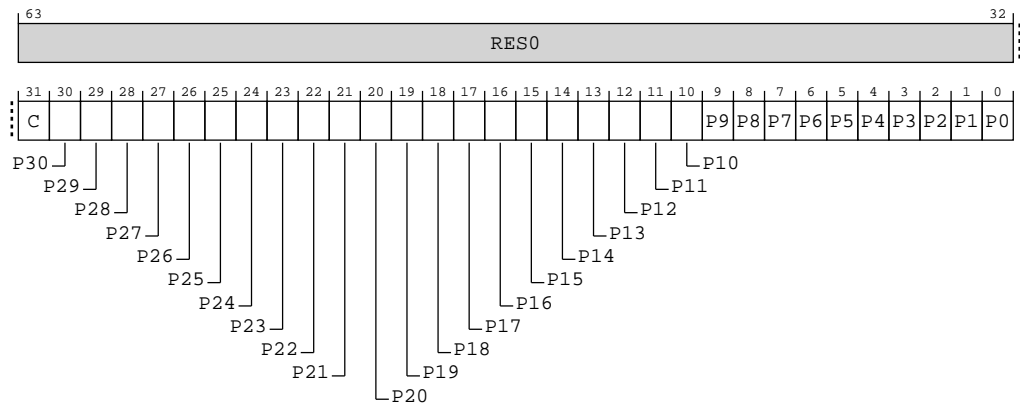


Table A-510: PMCNTENSET\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	AArch64-PMCCNTR_ELO enable. On writes, allows software to enable AArch64-PMCCNTR_ELO. On reads, returns the AArch64-PMCCNTR_ELO enable status.  <b>0b0</b> AArch64-PMCCNTR_ELO disabled.  <b>0b1</b> AArch64-PMCCNTR_ELO enabled.  Access to this field is W1S.	x

Bits	Name	Description	Reset
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>PMEVCNTR&lt;m&gt;_ELO enable. On writes, allows software to enable PMEVCNTR&lt;m&gt;_ELO. On reads, returns the PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL0 or EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1S.</li> </ul>	31 {x}

## Access

MRS <Xt>, PMCNTENSET\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b001

MSR PMCNTENSET\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b001

## Accessibility

MRS <Xt>, PMCNTENSET\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCNTENSET_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCNTENSET_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMCNTENSET_ELO;

```

MSR PMCNTESET\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCNTESET_ELO = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCNTESET_ELO = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMCNTESET_ELO = X[t, 64];
```

A.2.3.21 PMCNTECLR\_ELO, Performance Monitors Count Enable Clear Register

Disables the Cycle Count Register, AArch64-PMCCNTR\_ELO, and any implemented event counters AArch64-PMEVCNTR<n>\_ELO. Reading this register shows which counters are enabled.

Configurations

AArch64 register PMCNTECLR\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.10 PMCNTECLR\\_ELO, Performance Monitors Count Enable Clear Register](#) on page 2227 bits [31:0].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-190: AARCH64\_PMCNTENCLR\_ELO bit assignments

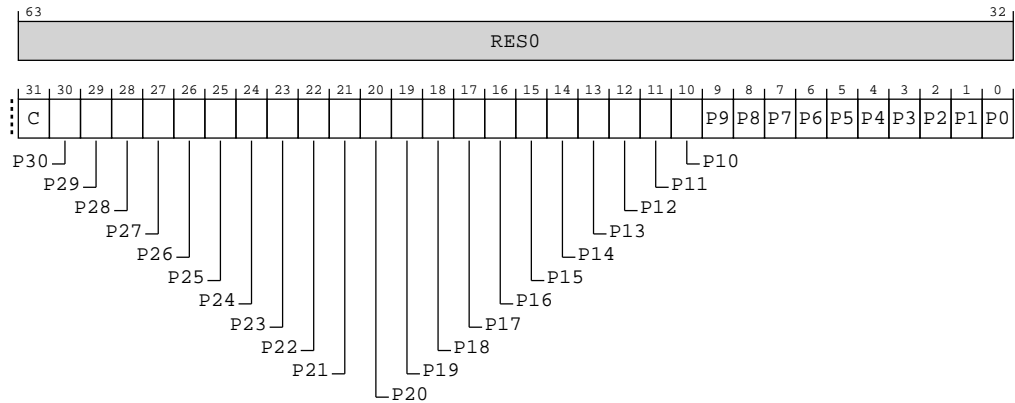


Table A-513: PMCNTENCLR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>AArch64-PMCCNTR_ELO disable. On writes, allows software to disable AArch64-PMCCNTR_ELO. On reads, returns the AArch64-PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>AArch64-PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>AArch64-PMCCNTR_ELO enabled.</p> <p>Access to this field is W1C.</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>PMEVCNTR&lt;m&gt;_ELO disable. On writes, allows software to disable PMEVCNTR&lt;m&gt;_ELO. On reads, returns the PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL0 or EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1C.</li> </ul>	31 {x}

## Access

MRS &lt;Xt&gt;, PMCNTENCLR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b010

MSR PMCNTENCLR\_ELO, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b010

## Accessibility

MRS &lt;Xt&gt;, PMCNTENCLR\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCNTENCLR_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCNTENCLR_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMCNTENCLR_ELO;

```

MSR PMCNTENCLR\_ELO, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCNTENCLR_ELO = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCNTENCLR_ELO = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMCNTENCLR_ELO = X[t, 64];

```

A.2.3.22 PMOVSCLR\_ELO, Performance Monitors Overflow Flag Status Clear Register

Contains the state of the overflow bit for the Cycle Count Register, AArch64-PMCCNTR\_ELO, and each of the implemented event counters AArch64-PMEVCNTR<n>\_ELO. Writing to this register clears these bits.

Configurations

AArch64 register PMOVSCLR\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.13 PMOVSCLR\\_ELO, Performance Monitors Overflow Flag Status Clear register](#) on page 2232 bits [31:0].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

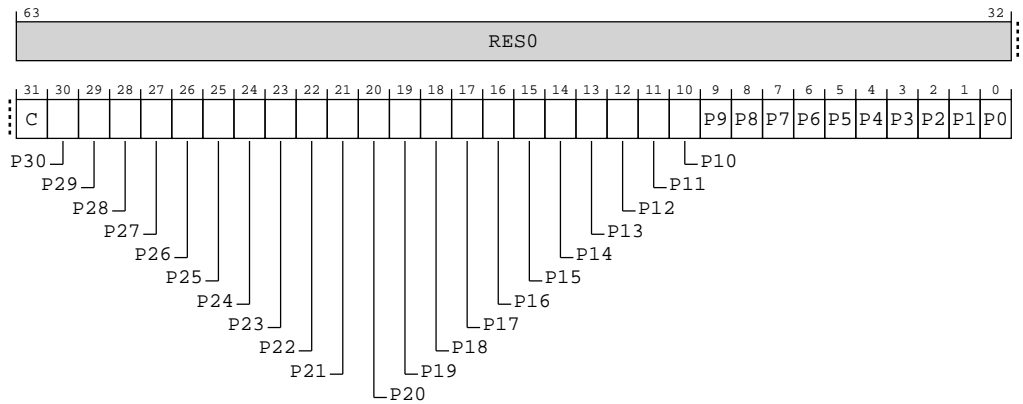


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-191: AARCH64\_PMOVSLR\_ELO bit assignments



**Table A-516: PMOVSLR\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	<p>Unsigned overflow flag for AArch64-PMCCNTR_ELO clear. On writes, allows software to clear the unsigned overflow flag for AArch64-PMCCNTR_ELO to 0. On reads, returns the unsigned overflow flag for AArch64-PMCCNTR_ELO overflow status.</p> <p><b>0b0</b> AArch64-PMCCNTR_ELO has not overflowed.</p> <p><b>0b1</b> AArch64-PMCCNTR_ELO has overflowed.</p> <p>Access to this field is W1C.</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO clear. On writes, allows software to clear the unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO to 0. On reads, returns the unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO overflow status.</p> <p><b>0b0</b> PMEVCNTR&lt;m&gt;_ELO has not overflowed.</p> <p><b>0b1</b> PMEVCNTR&lt;m&gt;_ELO has overflowed.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL0 or EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1C.</li> </ul>	31 {x}

### Access

MRS &lt;Xt&gt;, PMOVSLR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b011

MSR PMOVSLR\_ELO, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b011

### Accessibility

MRS &lt;Xt&gt;, PMOVSLR\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);

```



```

        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMOVSLR_EL0;
        elsif PSTATE.EL == EL1 then
            if MDCR_EL2.TPM == '1' then
                AArch64.SystemAccessTrap(EL2, 0x18);
            else
                X[t, 64] = PMOVSLR_EL0;
        elsif PSTATE.EL == EL2 then
            X[t, 64] = PMOVSLR_EL0;

```

MSR PMOVSLR\_EL0, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMOVSLR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMOVSLR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMOVSLR_EL0 = X[t, 64];

```

### A.2.3.23 PMSWINC\_EL0, Performance Monitors Software Increment Register

Increments a counter that is configured to count the Software increment event, event 0x00. For more information, see SW\_INCR in the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Configurations

AArch64 register PMSWINC\_EL0 bits [31:0] are architecturally mapped to External register [B.2.2.8.14 PMSWINC\\_EL0, Performance Monitors Software Increment Register](#) on page 2234 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

##### Reset value

```

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

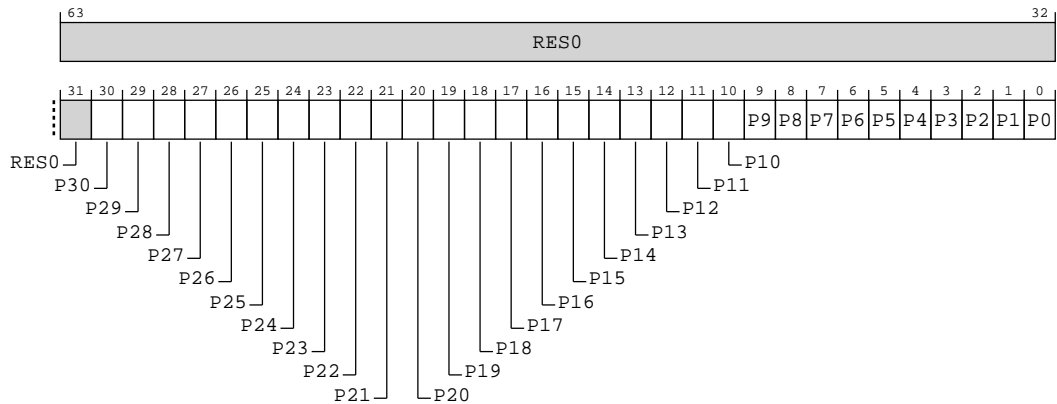
```



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-192: AARCH64\_PMSWINC\_ELO bit assignments**



**Table A-519: PMSWINC\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Software increment.</p> <p><b>0b0</b></p> <p>Write is ignored.</p> <p><b>0b1</b></p> <p>Increment PMEVCNTR&lt;m&gt;_ELO, if PMEVCNTR&lt;m&gt;_ELO is configured to count software increment events.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at ELO or EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is write-only.</li> </ul>	31 {x}

## Access

MSR PMSWINC\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b100

## Accessibility

MSR PMSWINC\_ELO, <Xt>

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.<SW,EN> == '00' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMSWINC_ELO = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMSWINC_ELO = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMSWINC_ELO = X[t, 64];

```

### A.2.3.24 PMSELR\_ELO, Performance Monitors Event Counter Selection Register

Selects the current event counter PMEVCNTR<n>\_EL1 or the cycle counter AArch32-PMCCNTR.

Used in conjunction with AArch64-PMXEVTYPER\_ELO to determine the event that increments a selected counter, and the modes and states in which the selected counter increments.

Used in conjunction with AArch64-PMXEVCNTR\_ELO to determine the value of a selected counter.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Performance Monitors registers

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-193: AARCH64\_PMSELR\_ELO bit assignments

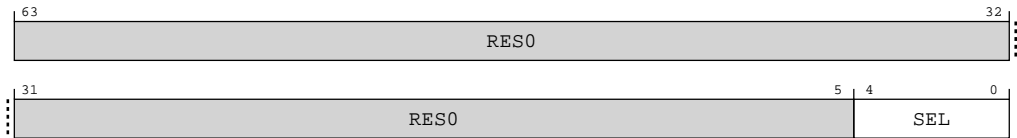


Table A-521: PMSELR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:5]	RES0	Reserved	RES0
[4:0]	SEL	Event counter select. Selects the counter accessed by subsequent accesses to AArch64-PMXEVTYPER_ELO and AArch64-PMXEVCNTR_ELO.  For more information about the results of accesses to the event counters, including when PMSELR_ELO.SEL is set to the index of an unimplemented or inaccessible event counter, see AArch64-PMXEVTYPER_ELO and AArch64-PMXEVCNTR_ELO.	5 {x}

Access

MRS <Xt>, PMSELR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b101

MSR PMSELR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b101

Accessibility

MRS <Xt>, PMSELR\_ELO

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.<ER,EN> == '00' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMSELR_ELO;
    elsif PSTATE.EL == EL1 then
```

```

    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMSELR_EL0;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMSELR_EL0;

```

MSR PMSELR\_EL0, &lt;Xt&gt;

```

    if PSTATE.EL == EL0 then
        if PMUSERENR_EL0.<ER,EN> == '00' then
            if HCR_EL2.TGE == '1' then
                AArch64.SystemAccessTrap(EL2, 0x18);
            else
                AArch64.SystemAccessTrap(EL1, 0x18);
            elsif MDCR_EL2.TPM == '1' then
                AArch64.SystemAccessTrap(EL2, 0x18);
            else
                PMSELR_EL0 = X[t, 64];
        elsif PSTATE.EL == EL1 then
            if MDCR_EL2.TPM == '1' then
                AArch64.SystemAccessTrap(EL2, 0x18);
            else
                PMSELR_EL0 = X[t, 64];
        elsif PSTATE.EL == EL2 then
            PMSELR_EL0 = X[t, 64];

```

### A.2.3.25 PMCEID0\_ELO, Performance Monitors Common Event Identification Register 0

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the ranges 0x0000 to 0x001F and 0x4000 to 0x401F.

For more information about the Common events and the use of the PMCEID<n>\_ELO registers see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Configurations

AArch64 register PMCEID0\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.18 PMCEID0, Performance Monitors Common Event Identification register 0](#) on page 2242 bits [31:0].

AArch64 register PMCEID0\_ELO bits [63:32] are architecturally mapped to External register [B.2.2.8.20 PMCEID2, Performance Monitors Common Event Identification register 2](#) on page 2252 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0100 0000 1111 1110 0011 1111 1111 1111 1111 1111

Bit descriptions

Figure A-194: AARCH64\_PMCEID0\_ELO bit assignments

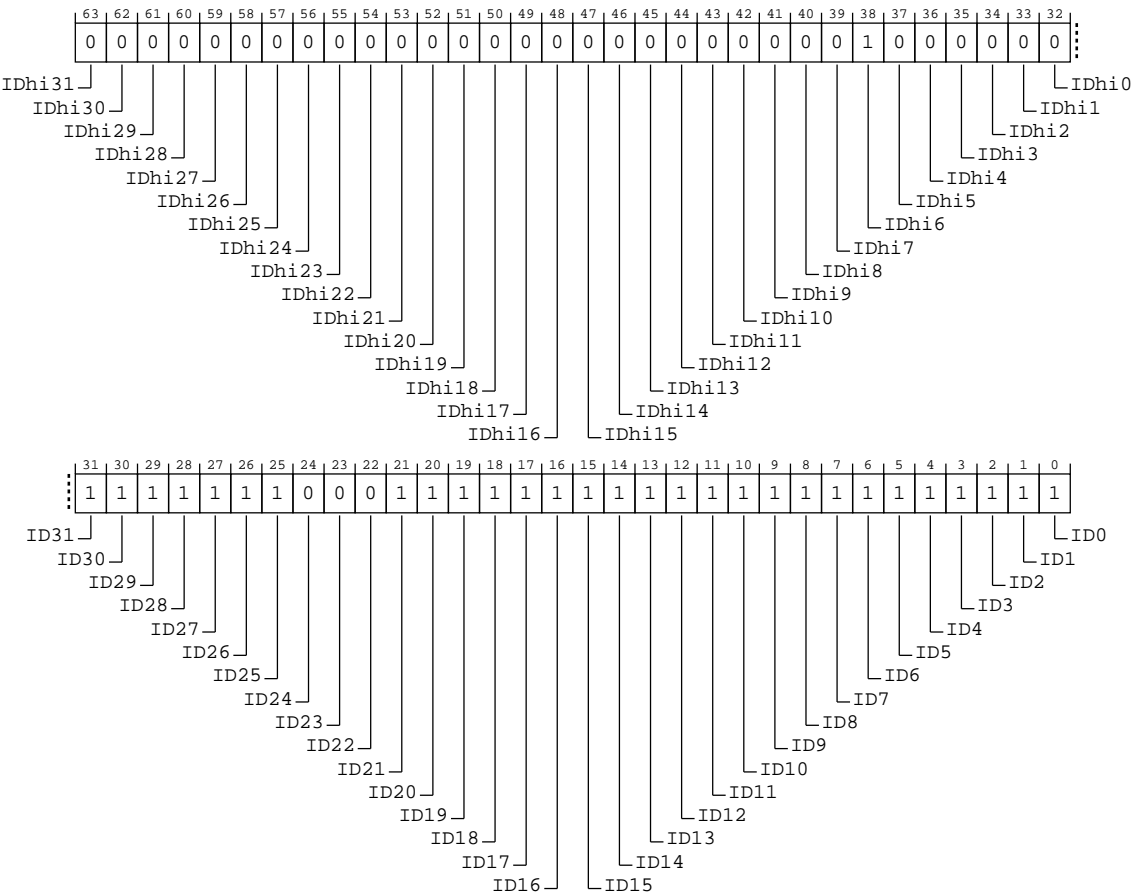


Table A-524: PMCEID0\_ELO bit descriptions

Bits	Name	Description	Reset
[63]	IDhi31	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b>  Event 0x401F not implemented.	0b0

Bits	Name	Description	Reset
[62]	IDHi30	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401E not implemented.	0b0
[61]	IDHi29	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401D not implemented.	0b0
[60]	IDHi28	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401C not implemented.	0b0
[59]	IDHi27	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401B not implemented.	0b0
[58]	IDHi26	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401A not implemented.	0b0
[57]	IDHi25	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4019 not implemented.	0b0
[56]	IDHi24	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4018 not implemented.	0b0
[55]	IDHi23	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4017 not implemented.	0b0
[54]	IDHi22	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4016 not implemented.	0b0

Bits	Name	Description	Reset
[53]	IDHi21	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4015 not implemented.	0b0
[52]	IDHi20	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4014 not implemented.	0b0
[51]	IDHi19	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4013 not implemented.	0b0
[50]	IDHi18	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4012 not implemented.	0b0
[49]	IDHi17	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4011 not implemented.	0b0
[48]	IDHi16	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4010 not implemented.	0b0
[47]	IDHi15	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400F not implemented.	0b0
[46]	IDHi14	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400E not implemented.	0b0
[45]	IDHi13	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400D not implemented.	0b0



Bits	Name	Description	Reset
[44]	IDHi12	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400C not implemented.	0b0
[43]	IDHi11	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400B not implemented.	0b0
[42]	IDHi10	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400A not implemented.	0b0
[41]	IDHi9	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4009 not implemented.	0b0
[40]	IDHi8	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4008 not implemented.	0b0
[39]	IDHi7	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4007 not implemented.	0b0
[38]	IDHi6	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b1</b> L1I_CACHE_LMISS event implemented.	0b1
[37]	IDHi5	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4005 not implemented.	0b0
[36]	IDHi4	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4004 not implemented.	0b0

Bits	Name	Description	Reset
[35]	IDhi3	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4003 not implemented.	0b0
[34]	IDhi2	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4002 not implemented.	0b0
[33]	IDhi1	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4001 not implemented.	0b0
[32]	IDhi0	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4000 not implemented.	0b0
[31]	ID31	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_ALLOCATE event implemented.	0b1
[30]	ID30	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CHAIN event implemented.	0b1
[29]	ID29	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BUS_CYCLES event implemented.	0b1
[28]	ID28	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> TTBR_WRITE_RETIRED event implemented.	0b1
[27]	ID27	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> INST_SPEC event implemented.	0b1

Bits	Name	Description	Reset
[26]	ID26	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> MEMORY_ERROR event implemented.	0b1
[25]	ID25	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BUS_ACCESS event implemented.	0b1
[24]	ID24	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0018 not implemented.	0b0
[23]	ID23	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0017 not implemented.	0b0
[22]	ID22	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0016 not implemented.	0b0
[21]	ID21	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_WB event implemented.	0b1
[20]	ID20	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_CACHE event implemented.	0b1
[19]	ID19	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> MEM_ACCESS event implemented.	0b1
[18]	ID18	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_PRED event implemented.	0b1

Bits	Name	Description	Reset
[17]	ID17	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CPU_CYCLES event implemented.	0b1
[16]	ID16	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_MIS_PRED event implemented.	0b1
[15]	ID15	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> UNALIGNED_LDST_RETIRED event implemented.	0b1
[14]	ID14	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_RETURN_RETIRED event implemented.	0b1
[13]	ID13	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_IMMED_RETIRED event implemented.	0b1
[12]	ID12	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> PC_WRITE_RETIRED event implemented.	0b1
[11]	ID11	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CID_WRITE_RETIRED event implemented.	0b1
[10]	ID10	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> EXC_RETURN event implemented.	0b1
[9]	ID9	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> EXC_TAKEN event implemented.	0b1

Bits	Name	Description	Reset
[8]	ID8	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> INST_RETIRED event implemented.	0b1
[7]	ID7	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> ST_RETIRED event implemented.	0b1
[6]	ID6	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> LD_RETIRED event implemented.	0b1
[5]	ID5	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_TLB_REFILL event implemented.	0b1
[4]	ID4	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE event implemented.	0b1
[3]	ID3	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_REFILL event implemented.	0b1
[2]	ID2	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_TLB_REFILL event implemented.	0b1
[1]	ID1	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_CACHE_REFILL event implemented.	0b1
[0]	ID0	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> SW_INCR event implemented.	0b1

## Access

MRS <Xt>, PMCEID0\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b110

## Accessibility

MRS <Xt>, PMCEID0\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCEID0_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCEID0_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMCEID0_ELO;

```

### A.2.3.26 PMCEID1\_ELO, Performance Monitors Common Event Identification Register 1

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the ranges 0x0020 to 0x003F and 0x4020 to 0x403F.

For more information about the Common events and the use of the PMCEID<n>\_ELO registers see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

AArch64 register PMCEID1\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.19 PMCEID1, Performance Monitors Common Event Identification register 1](#) on page 2247 bits [31:0].

AArch64 register PMCEID1\_ELO bits [63:32] are architecturally mapped to External register [B.2.2.8.21 PMCEID3, Performance Monitors Common Event Identification register 3](#) on page 2257 bits [31:0].

## Attributes

### Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0111 1111 1111 1100 0000 1010 0000 0111 1111

Bit descriptions

Figure A-195: AARCH64\_PMCEID1\_ELO bit assignments

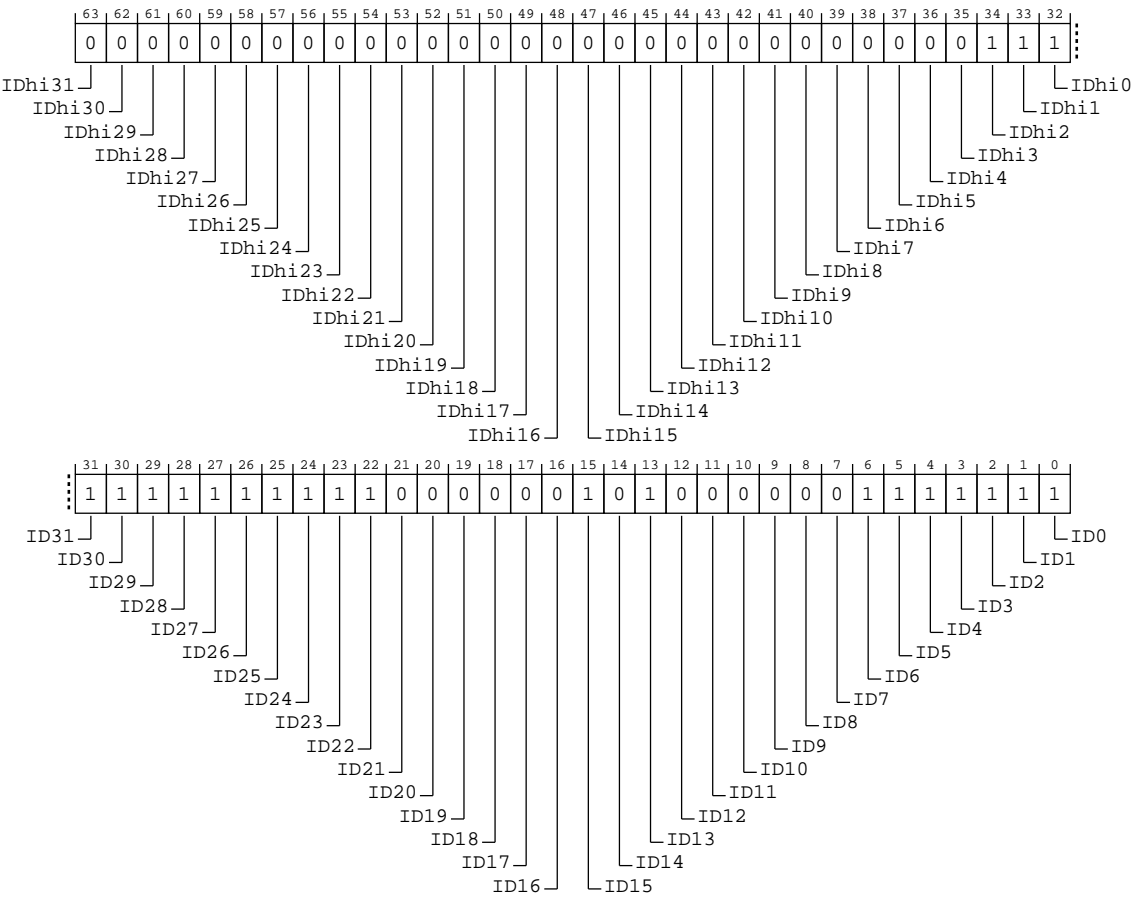


Table A-526: PMCEID1\_ELO bit descriptions

Bits	Name	Description	Reset
[63]	IDhi31	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b>  Event 0x403F not implemented.	0b0

Bits	Name	Description	Reset
[62]	IDHi30	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403E not implemented.	0b0
[61]	IDHi29	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403D not implemented.	0b0
[60]	IDHi28	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403C not implemented.	0b0
[59]	IDHi27	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403B not implemented.	0b0
[58]	IDHi26	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403A not implemented.	0b0
[57]	IDHi25	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4039 not implemented.	0b0
[56]	IDHi24	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4038 not implemented.	0b0
[55]	IDHi23	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4037 not implemented.	0b0
[54]	IDHi22	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4036 not implemented.	0b0



Bits	Name	Description	Reset
[53]	IDHi21	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4035 not implemented.	0b0
[52]	IDHi20	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4034 not implemented.	0b0
[51]	IDHi19	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4033 not implemented.	0b0
[50]	IDHi18	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4032 not implemented.	0b0
[49]	IDHi17	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4031 not implemented.	0b0
[48]	IDHi16	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4030 not implemented.	0b0
[47]	IDHi15	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402F not implemented.	0b0
[46]	IDHi14	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402E not implemented.	0b0
[45]	IDHi13	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402D not implemented.	0b0

Bits	Name	Description	Reset
[44]	IDHi12	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402C not implemented.	0b0
[43]	IDHi11	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402B not implemented.	0b0
[42]	IDHi10	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402A not implemented.	0b0
[41]	IDHi9	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4029 not implemented.	0b0
[40]	IDHi8	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4028 not implemented.	0b0
[39]	IDHi7	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4027 not implemented.	0b0
[38]	IDHi6	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4026 not implemented.	0b0
[37]	IDHi5	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4025 not implemented.	0b0
[36]	IDHi4	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4024 not implemented.	0b0

Bits	Name	Description	Reset
[35]	IDhi3	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4023 not implemented.	0b0
[34]	IDhi2	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> ST_ALIGN_LAT event implemented.	0b1
[33]	IDhi1	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> LD_ALIGN_LAT event implemented.	0b1
[32]	IDhi0	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> LDST_ALIGN_LAT event implemented.	0b1
[31]	ID31	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT event implemented.	0b1
[30]	ID30	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT_FRONTEND event implemented.	0b1
[29]	ID29	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT_BACKEND event implemented.	0b1
[28]	ID28	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL event implemented.	0b1
[27]	ID27	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> OP_SPEC event implemented.	0b1

Bits	Name	Description	Reset
[26]	ID26	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> OP_RETIRED event implemented.	0b1
[25]	ID25	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1D_CACHE_LMISS_RD event implemented.	0b1
[24]	ID24	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> REMOTE_ACCESS_RD event implemented.	0b1
[23]	ID23	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> LL_CACHE_MISS_RD event implemented.	0b1
[22]	ID22	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> LL_CACHE_RD event implemented.	0b1
[21]	ID21	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0035 not implemented.	0b0
[20]	ID20	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0034 not implemented.	0b0
[19]	ID19	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0033 not implemented.	0b0
[18]	ID18	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0032 not implemented.	0b0

Bits	Name	Description	Reset
[17]	ID17	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0031 not implemented.	0b0
[16]	ID16	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0030 not implemented.	0b0
[15]	ID15	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_TLB event implemented.	0b1
[14]	ID14	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002E not implemented.	0b0
[13]	ID13	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_TLB_REFILL event implemented.	0b1
[12]	ID12	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002C not implemented.	0b0
[11]	ID11	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002B not implemented.	0b0
[10]	ID10	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002A not implemented.	0b0
[9]	ID9	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0029 not implemented.	0b0

Bits	Name	Description	Reset
[8]	ID8	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0028 not implemented.	0b0
[7]	ID7	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0027 not implemented.	0b0
[6]	ID6	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1I_TLB event implemented.	0b1
[5]	ID5	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1D_TLB event implemented.	0b1
[4]	ID4	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_BACKEND event implemented.	0b1
[3]	ID3	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_FRONTEND event implemented.	0b1
[2]	ID2	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> BR_MIS_PRED_RETIRED event implemented.	0b1
[1]	ID1	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> BR_RETIRED event implemented.	0b1
[0]	ID0	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_CACHE_ALLOCATE event implemented.	0b1

## Access

MRS <Xt>, PMCEID1\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1100	0b111

## Accessibility

MRS <Xt>, PMCEID1\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCEID1_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCEID1_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMCEID1_ELO;

```

### A.2.3.27 PMCCNTR\_ELO, Performance Monitors Cycle Count Register

Holds the value of the processor Cycle Counter, CCNT, that counts processor clock cycles. See *Time as measured by the Performance Monitors cycle counter* in the [Arm® Architecture Reference Manual for A-profile architecture](#) for more information.

AArch64-PMCCFILTR\_ELO determines the modes and states in which the PMCCNTR\_ELO can increment.

## Configurations

All counters are subject to any changes in clock frequency, including clock stopping caused by the WFI and WFE instructions.

AArch64 register PMCCNTR\_ELO bits [63:0] are architecturally mapped to External register [B.2.2.8.2 PMCCNTR\\_ELO, Performance Monitors Cycle Counter](#) on page 2213 bits [63:0].

## Attributes

### Width

64

### Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-196: AARCH64\_PMCCNTR\_ELO bit assignments

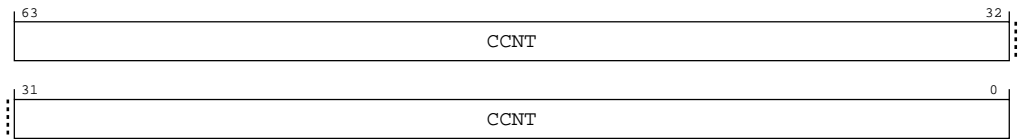


Table A-528: PMCCNTR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	CCNT	Cycle count. Depending on the values of AArch64-PMCR_ELO.{LC,D}, this field increments in one of the following ways: <ul style="list-style-type: none"><li>Every processor clock cycle.</li><li>Every 64th processor clock cycle.</li></ul> Writing 1 to AArch64-PMCR_ELO.C sets this field to 0.	64 {x}

Access

MRS <Xt>, PMCCNTR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b000

MSR PMCCNTR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b000

Accessibility

MRS <Xt>, PMCCNTR\_ELO

```
if PSTATE.EL == EL0 then
```



```

if PMUSERENR_EL0.<CR,EN> == '00' then
    if HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMCCNTR_EL0;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMCCNTR_EL0;
elsif PSTATE.EL == EL2 then
    X[t, 64] = PMCCNTR_EL0;

```

MSR PMCCNTR\_EL0, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCCNTR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCCNTR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMCCNTR_EL0 = X[t, 64];

```

### A.2.3.28 PMXEVTYPER\_EL0, Performance Monitors Selected Event Type Register

When AArch64-PMSELR\_EL0.SEL selects an event counter, this accesses a AArch64-PMEVTYPER<n>\_EL0 register. When AArch64-PMSELR\_EL0.SEL selects the cycle counter, this accesses AArch64-PMCCFILTR\_EL0.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

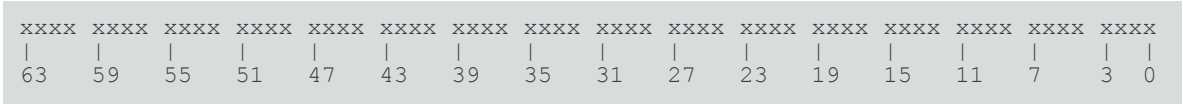
##### Functional group

Performance Monitors registers

##### Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-197: AArch64-PMXEVTYPYPER\_ELO bit assignments

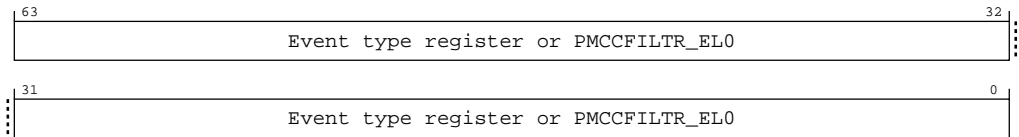


Table A-531: PMXEVTYPYPER\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	None	When AArch64-PMSELR_ELO.SEL == 31, this register accesses AArch64-PMCCFILTR_ELO.  Otherwise, this register accesses AArch64-PMEVTYPYPER<n>_ELO where n is the value in AArch64-PMSELR_ELO.SEL.	64 {x}

Access

If AArch64-PMSELR\_ELO.SEL is not 31, and is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMXEVTYPYPER\_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.

In ELO, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.EN.

If EL2 is implemented and enabled in the current Security state, in EL1 and ELO, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMXEVTYPYPER\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b001

MSR PMXEVTYPYPER\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b001

## Accessibility

If AArch64-PMSELR\_ELO.SEL is not 31, and is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMXEVTYPER\_ELO are CONSTRAINED UNPREDICTABLE, and the implemented behavior is: accesses to the register behave as RAZ/WI.

In EL0, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.EN.

If EL2 is implemented and enabled in the current Security state, in EL1 and EL0, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMXEVTYPER\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_ELO.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMXEVTYPER_ELO;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMXEVTYPER_ELO;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMXEVTYPER_ELO;

```

MSR PMXEVTYPER\_ELO, <Xt>

```

if PSTATE.EL == EL0 then
    if PMUSERENR_ELO.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMXEVTYPER_ELO = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMXEVTYPER_ELO = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMXEVTYPER_ELO = X[t, 64];

```

A.2.3.29 PMXEVCNTR\_ELO, Performance Monitors Selected Event Count Register

Reads or writes the value of the selected event counter, AArch64-PMXEVCNTR<n>\_ELO. AArch64-PMSELR\_ELO.SEL determines which event counter is selected.

Configurations

This register is available in all configurations.

Attributes

Width

64

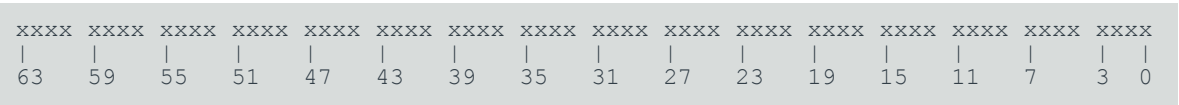
Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-198: AARCH64\_PMXEVCNTR\_ELO bit assignments

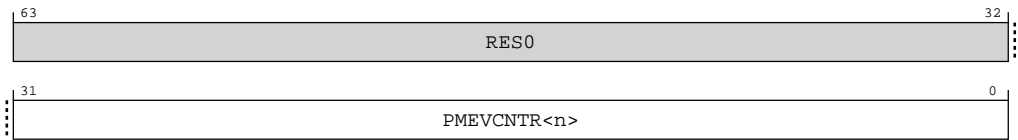


Table A-534: PMXEVCNTR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	PMXEVCNTR<n>	Value of the selected event counter, AArch64-PMXEVCNTR<n>_ELO, where n is the value stored in AArch64-PMSELR_ELO.SEL.	32 {x}

## Access

If AArch64-PMSELR\_ELO.SEL is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMXEVNTR\_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.

In EL0, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.{ER,EN}.

If EL2 is implemented and enabled in the current Security state, in EL1 and EL0, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMXEVNTR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b010

MSR PMXEVNTR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1101	0b010

## Accessibility

If AArch64-PMSELR\_ELO.SEL is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMXEVNTR\_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.

In EL0, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.{ER,EN}.

If EL2 is implemented and enabled in the current Security state, in EL1 and EL0, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMXEVNTR\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_ELO.<ER,EN> == '00' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMXEVNTR_ELO;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMXEVNTR_ELO;
elseif PSTATE.EL == EL2 then

```

```
X[t, 64] = PMXEVCNTR_ELO;
```

MSR PMXEVCNTR\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    if PMUSERENR_ELO.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMXEVCNTR_ELO = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMXEVCNTR_ELO = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMXEVCNTR_ELO = X[t, 64];
```

A.2.3.30 PMUSERENR\_ELO, Performance Monitors User Enable Register

Enables or disables ELO access to the Performance Monitors.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-199: AARCH64\_PMUSERENR\_ELO bit assignments

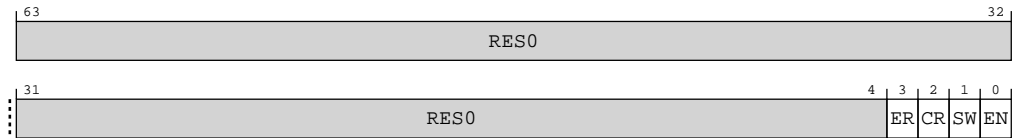


Table A-537: PMUSERENR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3]	ER	<p>Event counters Read enable.</p> <p>When PMUSERENR_ELO.EN is 0, PMUSERENR_ELO.ER enables ELO reads of the event counters and ELO reads and writes of the select register.</p> <p><b>0b0</b></p> <p>ELO reads of the event counters and ELO reads and writes of the select register are disabled, unless enabled by PMUSERENR_ELO.EN.</p> <p><b>0b1</b></p> <p>ELO reads of the event counters and ELO reads and writes of the select register are enabled, unless trapped by another control.</p> <p>In AArch64 state, the register accesses affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS reads of AArch64-PMEVCNTR&lt;n&gt;_ELO and AArch64-PMXVCNTR_ELO.</li> <li>MRS and MSR accesses to AArch64-PMSELR_ELO.</li> </ul> <p>When disabled, reads and writes generate an exception to EL1, or to EL2 when EL2 is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, and:</p> <ul style="list-style-type: none"> <li>AArch64 MRS and MSR accesses are reported using EC syndrome value 0x18.</li> </ul> <p>This field is ignored by the PE when PMUSERENR_ELO.EN == 1.</p>	x
[2]	CR	<p>Cycle counter Read enable.</p> <p>When PMUSERENR_ELO.EN is 0, PMUSERENR_ELO.CR enables ELO reads of the cycle counter.</p> <p><b>0b0</b></p> <p>ELO reads of the cycle counter are disabled, unless enabled by PMUSERENR_ELO.EN.</p> <p><b>0b1</b></p> <p>ELO reads of the cycle counter are enabled, unless trapped by another control.</p> <p>In AArch64 state, the register accesses affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS reads of AArch64-PMCCNTR_ELO.</li> </ul> <p>When disabled, reads generate an exception to EL1, or to EL2 when EL2 is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, and:</p> <ul style="list-style-type: none"> <li>AArch64 MRS reads are reported using EC syndrome value 0x18.</li> </ul> <p>This field is ignored by the PE when PMUSERENR_ELO.EN == 1.</p>	x

Bits	Name	Description	Reset
[1]	SW	<p>Software increment register Write enable.</p> <p>When PMUSERENR_ELO.EN is 0, PMUSERENR_ELO.SW enables ELO writes to the Software increment register.</p> <p><b>0b0</b></p> <p>ELO writes to the Software increment register are disabled, unless enabled by PMUSERENR_ELO.EN.</p> <p><b>0b1</b></p> <p>ELO writes to the Software increment register are enabled, unless trapped by another control.</p> <p>In AArch64 state, the register accesses affected by this control are:</p> <ul style="list-style-type: none"> <li>MSR writes to AArch64-PMSWINC_ELO.</li> </ul> <p>When disabled, writes generate an exception to EL1, or to EL2 when EL2 is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, and:</p> <ul style="list-style-type: none"> <li>AArch64 MSR writes are reported using EC syndrome value 0x18.</li> </ul> <p>This field is ignored by the PE when PMUSERENR_ELO.EN == 1.</p>	x
[0]	EN	<p>Enable.</p> <p>Enables ELO read/write access to PMU registers.</p> <p><b>0b0</b></p> <p>ELO accesses to the specified PMU System registers are trapped, unless enabled by PMUSERENR_ELO. {ER,CR,SW}.</p> <p><b>0b1</b></p> <p>ELO accesses to the specified PMU System registers are enabled, unless trapped by another control.</p> <p>In AArch64 state, the register accesses affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS or MSR accesses to AArch64-PMCCFILTR_ELO, AArch64-PMCCNTR_ELO, AArch64-PMCNTENCLR_ELO, AArch64-PMCNTENSET_ELO, AArch64-PMCR_ELO, AArch64-PMEVCNTR&lt;n&gt;_ELO, AArch64-PMEVTYPER&lt;n&gt;_ELO, AArch64-PMOVSCLR_ELO, AArch64-PMOVSSET_ELO, AArch64-PMSELR_ELO, AArch64-PMXVCNTR_ELO, and AArch64-PMXEVTYPER_ELO.</li> <li>MRS reads of AArch64-PMCEIDO_ELO and AArch64-PMCEID1_ELO.</li> <li>MSR writes to AArch64-PMSWINC_ELO.</li> </ul> <p>When trapped, reads and writes generate an exception to EL1, or to EL2 when EL2 is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, and:</p> <ul style="list-style-type: none"> <li>AArch64 MRS and MSR accesses are reported using EC syndrome value 0x18.</li> </ul>	x

## Access

MRS <Xt>, PMUSERENR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1110	0b000

MSR PMUSERENR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1110	0b000



Accessibility

MRS <Xt>, PMUSERENR\_ELO

```
if PSTATE.EL == EL0 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMUSERENR_ELO;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = PMUSERENR_ELO;
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMUSERENR_ELO;
```

MSR PMUSERENR\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMUSERENR_ELO = X[t, 64];
elseif PSTATE.EL == EL2 then
    PMUSERENR_ELO = X[t, 64];
```

A.2.3.31 PMOVSSET\_ELO, Performance Monitors Overflow Flag Status Set Register

Sets the state of the overflow bit for the Cycle Count Register, AArch64-PMCCNTR\_ELO, and each of the implemented event counters AArch64-PMEVCNTR<n>\_ELO.

Configurations

AArch64 register PMOVSSET\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.15 PMOVSSET\\_ELO, Performance Monitors Overflow Flag Status Set Register](#) on page 2236 bits [31:0].

Attributes

Width

64

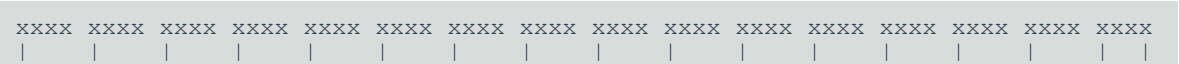
Functional group

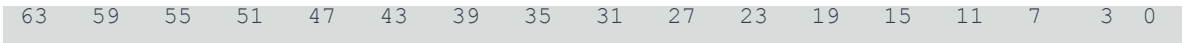
Performance Monitors registers

Access type

See bit descriptions

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-200: AArch64\_PMOVSET\_ELO bit assignments

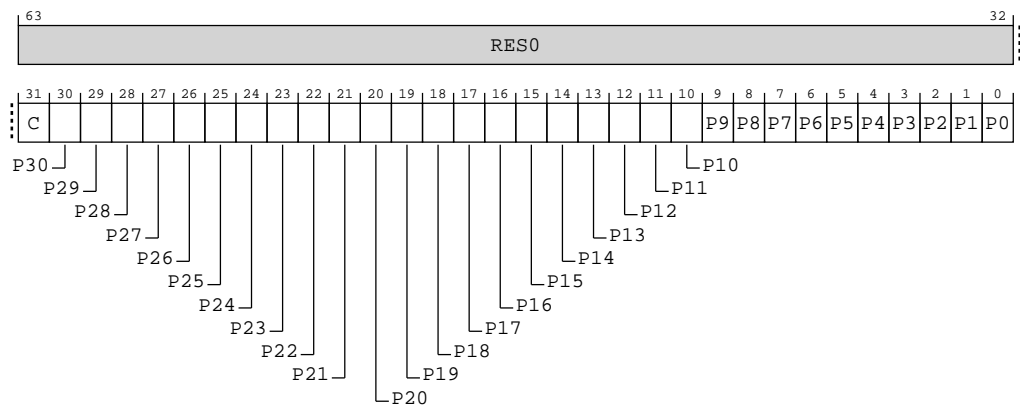


Table A-540: PMOVSET\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	C	Unsigned overflow flag for AArch64-PMCCNTR_ELO set. On writes, allows software to set the unsigned overflow flag for AArch64-PMCCNTR_ELO to 1. On reads, returns the unsigned overflow flag for AArch64-PMCCNTR_ELO overflow status.  <b>0b0</b> AArch64-PMCCNTR_ELO has not overflowed.  <b>0b1</b> AArch64-PMCCNTR_ELO has overflowed.  Access to this field is W1C.	x

Bits	Name	Description	Reset
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO set. On writes, allows software to set the unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO to 1. On reads, returns the unsigned overflow flag for PMEVCNTR&lt;m&gt;_ELO overflow status.</p> <p><b>0b0</b></p> <p>PMEVCNTR&lt;m&gt;_ELO has not overflowed.</p> <p><b>0b1</b></p> <p>PMEVCNTR&lt;m&gt;_ELO has overflowed.</p> <p>Accessing this field has the following behavior:</p> <ul style="list-style-type: none"> <li>This field reads-as-zero and ignores writes if any of the following are true: <ul style="list-style-type: none"> <li>All of the following are true: <ul style="list-style-type: none"> <li>EL2 is implemented and enabled in the current Security state.</li> <li>m &gt;= UInt(AArch64-MDCR_EL2.HPMN).</li> <li>Accessed at EL0 or EL1.</li> </ul> </li> <li>m &gt;= UInt(AArch64-PMCR_ELO.N).</li> </ul> </li> <li>Otherwise access to this field is W1S.</li> </ul>	31 {x}

## Access

MRS <Xt>, PMOVSSET\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1110	0b011

MSR PMOVSSET\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1001	0b1110	0b011

## Accessibility

MRS <Xt>, PMOVSSET\_ELO

```

if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elseif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMOVSSET_ELO;
    elseif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMOVSSET_ELO;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = PMOVSSET_ELO;

```

MSR PMOVSSET\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMOVSSET_EL0 = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMOVSSET_EL0 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMOVSSET_EL0 = X[t, 64];
```

A.2.3.32 PMEVCNTR<n>\_ELO, Performance Monitors Event Count Registers, n = 0 - 5

Holds event counter n, which counts events, where n is 0 to 30.

Configurations

AArch64 register PMEVCNTR<n>\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.8.1 PMEVCNTR<n>\\_ELO, Performance Monitors Event Count Registers, n = 0 - 5](#) on page 2212 bits [31:0].

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-201: AARCH64\_PMEVCNTR<n>\_ELO bit assignments

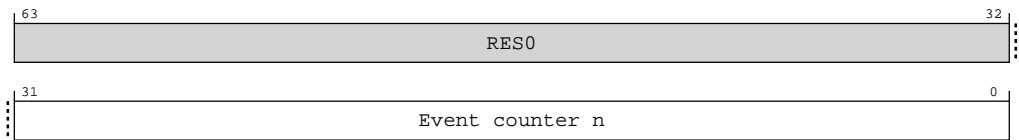


Table A-543: PMEVCNTR<n>\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	None	Event counter n. Value of event counter n, where n is the number of this register and is a number from 0 to 30.	32 {x}

Access

PMEVCNTR<n>\_ELO can also be accessed by using AArch64-PMXEVCNTR\_ELO with AArch64-PMSELR\_ELO.SEL set to the value of <n>.

If <n> is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMEVCNTR<n>\_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.



In ELO, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO. {ER,EN}.

If EL2 is implemented and enabled in the current Security state, in EL1 and ELO, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMEVCNTR<m>\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	'10':m[4:3]	m[2:0]

MSR PMEVCNTR<m>\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	'10':m[4:3]	m[2:0]

Accessibility

PMEVCNTR<n>\_ELO can also be accessed by using AArch64-PMXEVCNTR\_ELO with AArch64-PMSELR\_ELO.SEL set to the value of <n>.

If <n> is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMUVCNTR<n>\_ELO are CONSTRAINED UNPREDICTABLE, and the implemented behavior is: accesses to the register behave as RAZ/WI.



In ELO, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.  
{ER,EN}.

If EL2 is implemented and enabled in the current Security state, in EL1 and ELO, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS <Xt>, PMUVCNTR<m>\_ELO

```
integer m = UInt(CRm<1:0>:op2<2:0>);

if m >= 6 then
    ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
elseif PSTATE.EL == EL0 then
    if PMUSERENR_EL0.<ER,EN> == '00' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif m >= AArch64.GetNumEventCountersAccessible() then
        ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
    else
        X[t, 64] = PMUVCNTR_EL0[m];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif m >= AArch64.GetNumEventCountersAccessible() then
        ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
    else
        X[t, 64] = PMUVCNTR_EL0[m];
elseif PSTATE.EL == EL2 then
    X[t, 64] = PMUVCNTR_EL0[m];
```

MSR PMUVCNTR<m>\_ELO, <Xt>

```
integer m = UInt(CRm<1:0>:op2<2:0>);

if m >= 6 then
    ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
elseif PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif m >= AArch64.GetNumEventCountersAccessible() then
        ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
    else
        PMUVCNTR_EL0[m] = X[t, 64];
elseif PSTATE.EL == EL1 then
```

```
if MDCR_EL2.TPM == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
elsif m >= AArch64.GetNumEventCountersAccessible() then
    ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
else
    PMEVCNTR_EL0[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    PMEVCNTR_EL0[m] = X[t, 64];
```

A.2.3.33 PMEVTYPER<n>\_ELO, Performance Monitors Event Type Registers, n = 0 - 5

Configures event counter n, where n is 0 to 30.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value

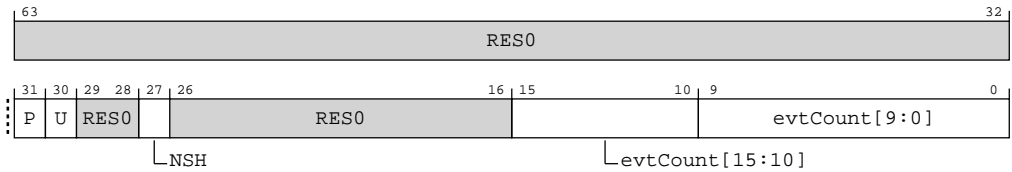
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-202: AARCH64\_PMEVTYPER<n>\_ELO bit assignments



**Table A-546: PMEVTYPER<n>\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	P	EL1 filtering. Controls counting events in EL1.  <b>0b0</b> This field has no effect on filtering of events.  <b>0b1</b> Events in EL1 are not counted.	x
[30]	U	ELO filtering. Controls counting events in ELO.  <b>0b0</b> This field has no effect on filtering of events.  <b>0b1</b> Events in ELO are not counted.	x
[29:28]	RES0	Reserved	RES0
[27]	NSH	EL2 filtering. Controls counting events in EL2.  <b>0b0</b> Events in EL2 are not counted.  <b>0b1</b> This field has no effect on filtering of events.	x
[26:16]	RES0	Reserved	RES0
[15:10]	evtCount[15:10]	Extension to evtCount[9:0]. For more information, see evtCount[9:0].	6 {x}
[9:0]	evtCount[9:0]	Event to count.  The event number of the event that is counted by event counter AArch64-PMEVCNTR<n>_ELO.  The ranges of event numbers allocated to each type of event are shown in <i>Allocation of the PMU event number space</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .  If PMEVTYPER<n>_ELO.evtCount is programmed to an event that is reserved or not supported by the PE, the behavior depends on the value written: <ul style="list-style-type: none"> <li>For the range 0x0000 to 0x003F, no events are counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is the value written to the field.</li> <li>If FEAT_PMUv3p1 is implemented, for the range 0x4000 to 0x403F, no events are counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is the value written to the field.</li> <li>For other values, it is UNPREDICTABLE what event, if any, is counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is <b>UNKNOWN</b>.</li> </ul> <b>Note:</b> UNPREDICTABLE means the event must not expose privileged information.	10 {x}

## Access

PMEVTYPER<n>\_ELO can also be accessed by using AArch64-PMXEVTYPER\_ELO with AArch64-PMSELR\_ELO.SEL set to n.



If  $\langle n \rangle$  is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMEVTYPER $\langle n \rangle$ \_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.



In ELO, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.EN.

If EL2 is implemented and enabled in the current Security state, in EL1 and ELO, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS  $\langle Xt \rangle$ , PMEVTYPER $\langle m \rangle$ \_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	'11':m[4:3]	m[2:0]

MSR PMEVTYPER $\langle m \rangle$ \_ELO,  $\langle Xt \rangle$

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	'11':m[4:3]	m[2:0]

### Accessibility

PMEVTYPER $\langle n \rangle$ \_ELO can also be accessed by using AArch64-PMXEVTYPER\_ELO with AArch64-PMSELR\_ELO.SEL set to  $n$ .

If  $\langle n \rangle$  is greater than or equal to the number of accessible event counters, then reads and writes of AArch64-PMEVTYPER $\langle n \rangle$ \_ELO are **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is: accesses to the register behave as RAZ/WI.



In ELO, an access is permitted if it is enabled by AArch64-PMUSERENR\_ELO.EN.

If EL2 is implemented and enabled in the current Security state, in EL1 and ELO, AArch64-MDCR\_EL2.HPMN identifies the number of accessible event counters. Otherwise, the number of accessible event counters is the number of implemented event counters. For more information, see AArch64-MDCR\_EL2.HPMN.

MRS  $\langle Xt \rangle$ , PMEVTYPER $\langle m \rangle$ \_ELO

```
integer m = UInt(CRm<1:0>:op2<2:0>);
if m >= 6 then
    ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
```

```

elseif PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elseif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elseif m >= AArch64.GetNumEventCountersAccessible() then
            ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
        else
            X[t, 64] = PMEVTYPER_EL0[m];
    elseif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elseif m >= AArch64.GetNumEventCountersAccessible() then
            ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
        else
            X[t, 64] = PMEVTYPER_EL0[m];
    elseif PSTATE.EL == EL2 then
        X[t, 64] = PMEVTYPER_EL0[m];

```

MSR PMEVTYPER<m>\_EL0, <Xt>

```

integer m = UInt(CRm<1:0>:op2<2:0>);

if m >= 6 then
    ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
elseif PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elseif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elseif m >= AArch64.GetNumEventCountersAccessible() then
            ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
        else
            PMEVTYPER_EL0[m] = X[t, 64];
    elseif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        elseif m >= AArch64.GetNumEventCountersAccessible() then
            ConstrainUnpredictableProcedure(Unpredictable_PMUEVENTCOUNTER);
        else
            PMEVTYPER_EL0[m] = X[t, 64];
    elseif PSTATE.EL == EL2 then
        PMEVTYPER_EL0[m] = X[t, 64];

```

### A.2.3.34 PMCCFILTR\_EL0, Performance Monitors Cycle Count Filter Register

Determines the modes in which the Cycle Counter, AArch64-PMCCNTR\_EL0, increments.

#### Configurations

AArch64 register PMCCFILTR\_EL0 bits [31:0] are architecturally mapped to External register [B.2.2.8.8 PMCCFILTR\\_EL0, Performance Monitors Cycle Counter Filter Register](#) on page 2223 bits [31:0].

Attributes

Width

64

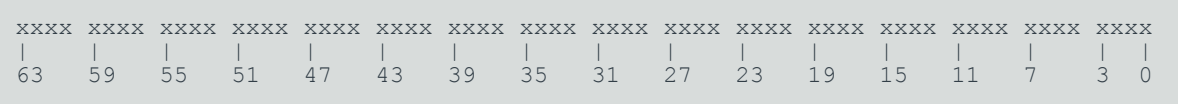
Functional group

Performance Monitors registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-203: AARCH64\_PMCCFILTR\_EL0 bit assignments

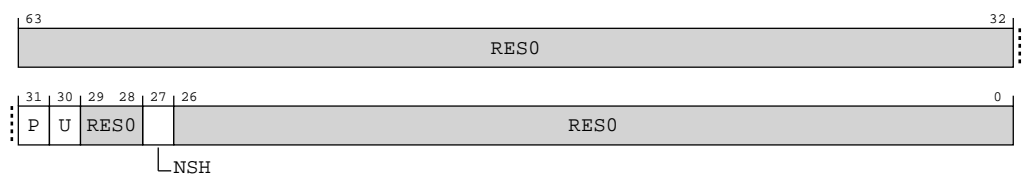


Table A-549: PMCCFILTR\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	P	EL1 filtering. Controls counting cycles in EL1. <b>0b0</b> This field has no effect on filtering of cycles. <b>0b1</b> Cycles in EL1 are not counted.	x
[30]	U	ELO filtering. Controls counting cycles in ELO. <b>0b0</b> This field has no effect on filtering of cycles. <b>0b1</b> Cycles in ELO are not counted.	x
[29:28]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[27]	NSH	EL2 filtering. Controls counting cycles in EL2.  <b>0b0</b> Cycles in EL2 are not counted.  <b>0b1</b> This field has no effect on filtering of cycles.	x
[26:0]	RES0	Reserved	RES0

Access

PMCCFILTR\_ELO can also be accessed by using AArch64-PMXEVTYPER\_ELO with AArch64-PMSELR\_ELO.SEL set to 0b11111.

MRS <Xt>, PMCCFILTR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b1111	0b111

MSR PMCCFILTR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b1111	0b111

Accessibility

PMCCFILTR\_ELO can also be accessed by using AArch64-PMXEVTYPER\_ELO with AArch64-PMSELR\_ELO.SEL set to 0b11111.

MRS <Xt>, PMCCFILTR\_ELO

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCCFILTR_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PMCCFILTR_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = PMCCFILTR_ELO;
```

MSR PMCCFILTR\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    if PMUSERENR_EL0.EN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
```

```
    elsif MDCR_EL2.TPM == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        PMCCFILTR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.TPM == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            PMCCFILTR_EL0 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        PMCCFILTR_EL0 = X[t, 64];
```

## A.2.4 AArch64 System instruction register description

This section includes the register descriptions for all System instruction registers in the Cortex®-R82AE processor.

### A.2.4.1 IC IALLUIS, Instruction Cache Invalidate All to PoU, Inner Shareable

Invalidate all instruction caches in the Inner Shareable domain of the PE executing the instruction to the Point of Unification.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

System instructions

#### Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

IC IALLUIS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b0001	0b000

#### Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

IC IALLUIS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TPU == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.IC(CacheOpScope_ALLUIS);
elsif PSTATE.EL == EL2 then
    AArch64.IC(CacheOpScope_ALLUIS);
```

A.2.4.2 IC IALLU, Instruction Cache Invalidate All to PoU

Invalidate all instruction caches of the PE executing the instruction to the Point of Unification.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

IC IALLU{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b0101	0b000

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

IC IALLU{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TPU == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FB == '1' then
        AArch64.IC(CacheOpScope_ALLUIS);
```

```
else
    AArch64.IC(CacheOpScope_ALLU);
elseif PSTATE.EL == EL2 then
    AArch64.IC(CacheOpScope_ALLU);
```

A.2.4.3 DC IVAC, Data or unified Cache line Invalidate by VA to PoC

Invalidate data cache by address to Point of Coherency.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-204: AARCH64\_DC\_IVAC bit assignments

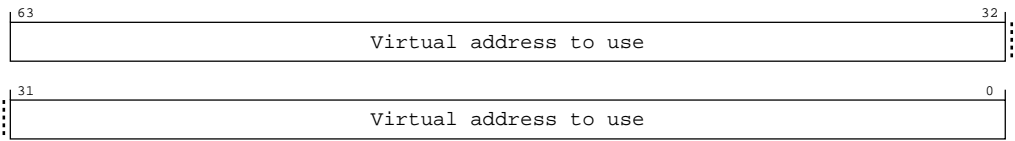


Table A-554: DC IVAC bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 {x}

Access

When the instruction is executed, it can generate a watchpoint, which is prioritized in the same way as other watchpoints. If a watchpoint is generated, the CM bit in the ESR\_ELx.ISS field is set to 1.

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC IVAC, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b0110	0b001

### Accessibility

When the instruction is executed, it can generate a watchpoint, which is prioritized in the same way as other watchpoints. If a watchpoint is generated, the CM bit in the ESR\_ELx.ISS field is set to 1.

If ELO access is enabled, when executed at EL0, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC IVAC, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TPCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Invalidate, CacheOpScope_PoC);
elsif PSTATE.EL == EL2 then
    AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Invalidate, CacheOpScope_PoC);

```

#### A.2.4.4 DC ISW, Data or unified Cache line Invalidate by Set/Way

Invalidate data cache by set/way.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions



Bit descriptions

Figure A-205: AARCH64\_DC\_ISW bit assignments

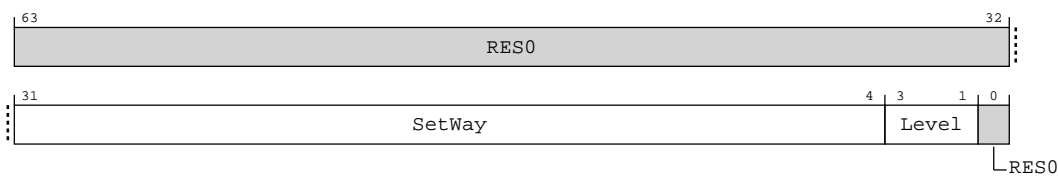


Table A-556: DC ISW bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:4]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:32-A], the number of the way to operate on.</li><li>Set, bits[B-1:L], the number of the set to operate on.</li></ul> Bits[L-1:4] are <b>RES0</b> .  $A = \text{Log}_2(\text{ASSOCIATIVITY})$ , $L = \text{Log}_2(\text{LINELEN})$ , $B = (L + S)$ , $S = \text{Log}_2(\text{NSETS})$ .  ASSOCIATIVITY, LINELEN (line length, in bytes), and NSETS (number of sets) have their usual meanings and are the values for the cache level being operated on. The values of A and S are rounded up to the next integer.	28 {x}
[3:1]	Level	Cache level to operate on, minus 1. For example, this field is 0 for operations on L1 cache, or 1 for operations on L2 cache.	xxx
[0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC ISW, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b0110	0b010

Accessibility

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC ISW, <Xt>

```
if PSTATE.EL == EL0 then
```

```
    UNDEFINED;
  elseif PSTATE.EL == EL1 then
    if HCR_EL2.TSW == '1' then
      AArch64.SystemAccessTrap(EL2, 0x18);
    else
      AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Invalidate,
        CacheOpScope_SetWay);
    elseif PSTATE.EL == EL2 then
      AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Invalidate, CacheOpScope_SetWay);
```

A.2.4.5 AT S1E1R, Address Translate Stage 1 EL1 Read

Performs stage 1 address translation, with permissions as if reading from the given virtual address from EL1, using the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-206: AARCH64\_AT\_S1E1R bit assignments

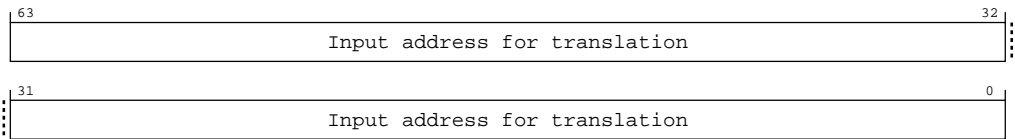


Table A-558: AT S1E1R bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1E1R, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1000	0b000

Accessibility

AT S1E1R, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Read);
elsif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Read);
```

A.2.4.6 AT S1E1W, Address Translate Stage 1 EL1 Write

Performs stage 1 address translation, with permissions as if writing to the given virtual address from EL1, using the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-207: AARCH64\_AT\_S1E1W bit assignments

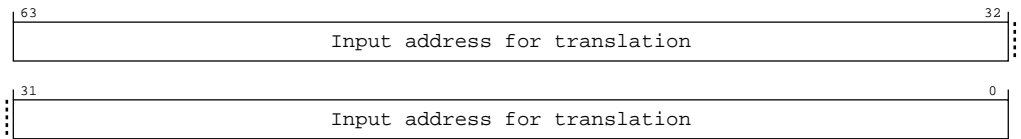


Table A-560: AT S1E1W bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1E1W, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1000	0b001

Accessibility

AT S1E1W, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Write);
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Write);
```

A.2.4.7 AT S1EOR, Address Translate Stage 1 ELO Read

Performs stage 1 address translation from ELO, with permissions as if reading from the given virtual address from ELO, using the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-208: AARCH64\_AT\_S1EOR bit assignments

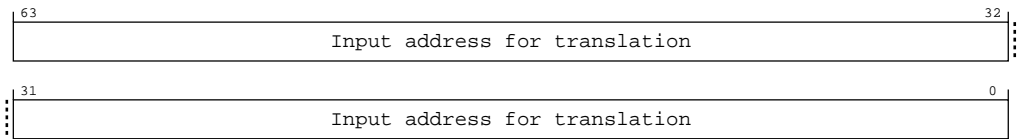


Table A-562: AT S1EOR bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1EOR, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1000	0b010

Accessibility

AT S1EOR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Read);
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Read);
```

A.2.4.8 AT S1EOW, Address Translate Stage 1 ELO Write

Performs stage 1 address translation from ELO, with permissions as if writing to the given virtual address from ELO, using the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-209: AARCH64\_AT\_S1EOW bit assignments

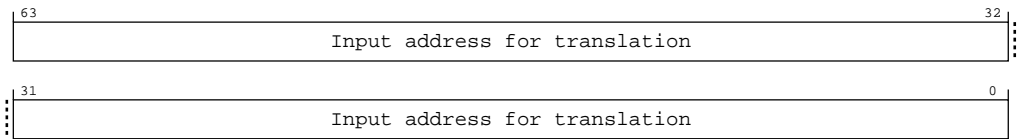


Table A-564: AT S1EOW bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1EOW, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1000	0b011

Accessibility

AT S1E0W, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Write);
elsif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Write);
```

A.2.4.9 AT S1E1RP, Address Translate Stage 1 EL1 Read PAN

Performs a stage 1 address translation, where the value of PSTATE.PAN determines if a read from a location will generate a Permission fault for a privileged access, using the EL1&0 translation regime, accessed from EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-210: AARCH64\_AT\_S1E1RP bit assignments

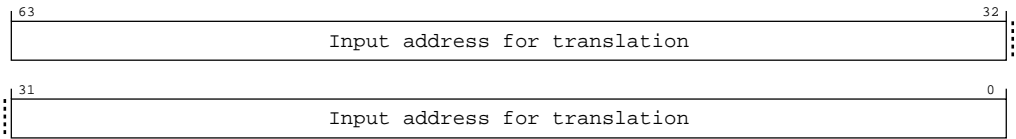


Table A-566: AT S1E1RP bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1E1RP, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1001	0b000

Accessibility

AT S1E1RP, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_ReadPAN);
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_ReadPAN);
```

A.2.4.10 AT S1E1WP, Address Translate Stage 1 EL1 Write PAN

Performs a stage 1 address translation, where the value of PSTATE.PAN determines if a write to a location will generate a Permission fault for a privileged access, using the EL1&0 translation regime, accessed from EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-211: AARCH64\_AT\_S1E1WP bit assignments

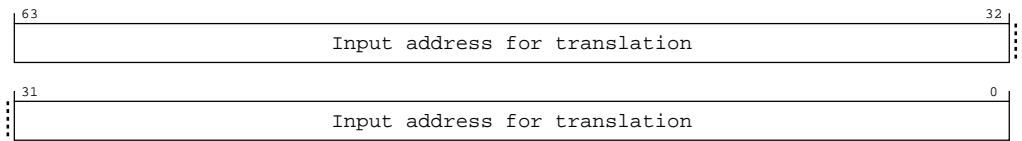


Table A-568: AT S1E1WP bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1E1WP, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1001	0b001

Accessibility

AT S1E1WP, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_WritePAN);
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_WritePAN);
```

A.2.4.11 DC CSW, Data or unified Cache line Clean by Set/Way

Clean data cache by set/way.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-212: AARCH64\_DC\_CSW bit assignments

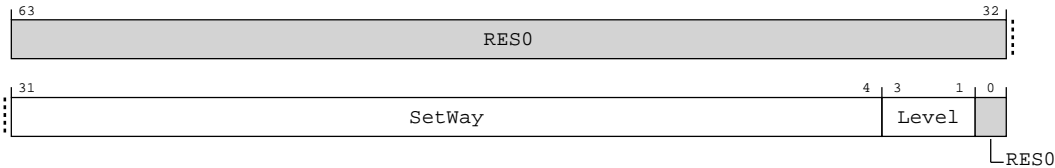


Table A-570: DC CSW bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[31:4]	SetWay	<p>Contains two fields:</p> <ul style="list-style-type: none"> <li>Way, bits[31:32-A], the number of the way to operate on.</li> <li>Set, bits[B-1:L], the number of the set to operate on.</li> </ul> <p>Bits[L-1:4] are <b>RES0</b>.</p> <p><math>A = \text{Log}_2(\text{ASSOCIATIVITY})</math>, <math>L = \text{Log}_2(\text{LINELEN})</math>, <math>B = (L + S)</math>, <math>S = \text{Log}_2(\text{NSETS})</math>.</p> <p>ASSOCIATIVITY, LINELEN (line length, in bytes), and NSETS (number of sets) have their usual meanings and are the values for the cache level being operated on. The values of A and S are rounded up to the next integer.</p>	28 {x}
[3:1]	Level	Cache level to operate on, minus 1. For example, this field is 0 for operations on L1 cache, or 1 for operations on L2 cache.	xxx
[0]	RES0	Reserved	RES0

## Access

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC CSW, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1010	0b010

## Accessibility

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC CSW, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TSW == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_SetWay);
elsif PSTATE.EL == EL2 then
    AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_SetWay);

```

A.2.4.12 DC CISW, Data or unified Cache line Clean and Invalidate by Set/Way

Clean and Invalidate data cache by set/way.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-213: AARCH64\_DC\_CISW bit assignments

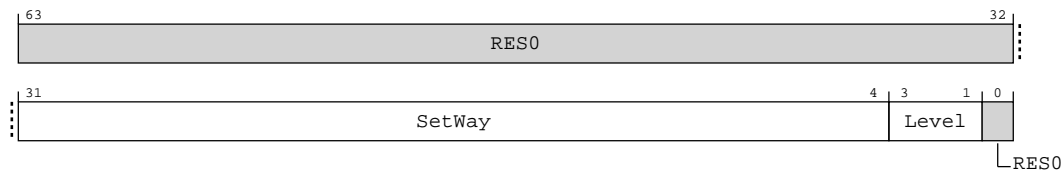


Table A-572: DC CISW bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:4]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:32-A], the number of the way to operate on.</li><li>Set, bits[B-1:L], the number of the set to operate on.</li></ul> Bits[L-1:4] are RES0.  $A = \text{Log}_2(\text{ASSOCIATIVITY})$ , $L = \text{Log}_2(\text{LINELEN})$ , $B = (L + S)$ , $S = \text{Log}_2(\text{NSETS})$ .  ASSOCIATIVITY, LINELEN (line length, in bytes), and NSETS (number of sets) have their usual meanings and are the values for the cache level being operated on. The values of A and S are rounded up to the next integer.	28 {x}
[3:1]	Level	Cache level to operate on, minus 1. For example, this field is 0 for operations on L1 cache, or 1 for operations on L2 cache.	xxx
[0]	RES0	Reserved	RES0

## Access

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC C1SW, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b000	0b0111	0b1110	0b010

## Accessibility

If this instruction is executed with a set, way or level argument that is larger than the value supported by the implementation then the behavior is **CONSTRAINED UNPREDICTABLE** and the implemented behavior is:

- The instruction performs cache maintenance on a single arbitrary cache line.

DC C1SW, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TSW == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_CleanInvalidate,
        CacheOpScope_SetWay);
    elseif PSTATE.EL == EL2 then
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_CleanInvalidate,
        CacheOpScope_SetWay);
```

### A.2.4.13 TLBI VMALLE1OS, TLB Invalidate by VMID, All at stage 1, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.



When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

## Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b000

## Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBI_AllAttr);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBI_AllAttr);

```

#### A.2.4.14 TLBI VAE1OS, TLB Invalidate by VA, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

---

When



**Note**

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.
- 

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

Bit descriptions

Figure A-214: AARCH64\_TLBI\_VAE1OS bit assignments

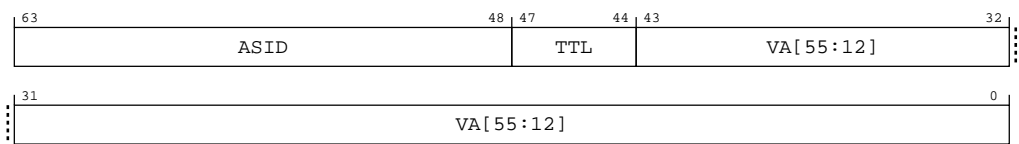


Table A-575: TLBI VAE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b001

Accessibility

TLBI VAE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.15 TLBI ASIDE1OS, TLB Invalidate by ASID, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used for the specified ASID, and either:
  - Is from a level of lookup above the final level.
  - Is a non-global entry from the final level of lookup.

The entry would be used with the current VMID and would be required to translate an address using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions



Access type

See bit descriptions

Bit descriptions

Figure A-215: AARCH64\_TLBI\_ASIDE1OS bit assignments

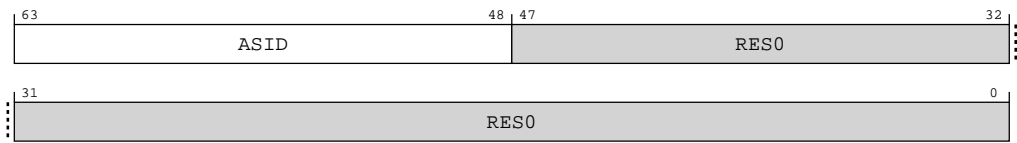


Table A-577: TLBI ASIDE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any appropriate TLB entries that match the ASID values will be affected by this System instruction.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}
[47:0]	RES0	Reserved	RES0

Access

TLBI ASIDE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b010

Accessibility

TLBI ASIDE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBI_AllAttr, X[t, 64]);
```

A.2.4.16 TLBI VAAE1OS, TLB Invalidate by VA, All ASID, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When



a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.



For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-216: AARCH64\_TLBI\_VAAE1OS bit assignments

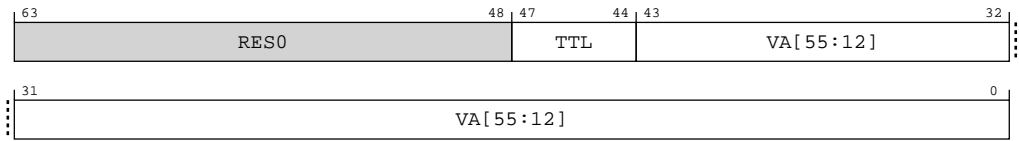


Table A-579: TLBI VAAE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAAE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b011

Accessibility

TLBI VAAE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
        TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.17 TLBI VALE1OS, TLB Invalidate by VA, Last level, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When



Note

- a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:
- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-217: AARCH64\_TLBI\_VALE1OS bit assignments

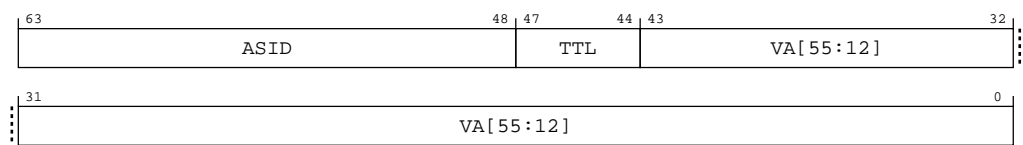


Table A-581: TLBI VALE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VALE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b101

Accessibility

TLBI VALE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```

A.2.4.18 TLBI VAALE1OS, TLB Invalidate by VA, All ASID, Last Level, EL1, Outer Shareable


Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the final level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.


When



Note

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-218: AARCH64\_TLBI\_VAALE1OS bit assignments

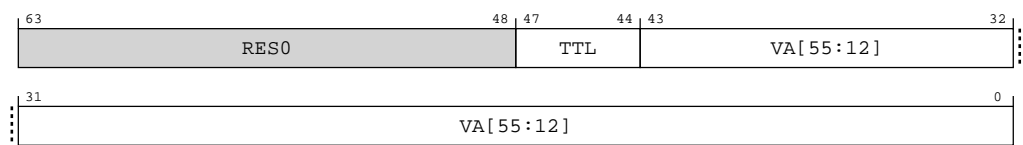


Table A-583: TLBI VAALE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAALE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0001	0b111

Accessibility

TLBI VAALE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
```

A.2.4.19 TLBI RVAE1IS, TLB Range Invalidate by VA, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 00000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

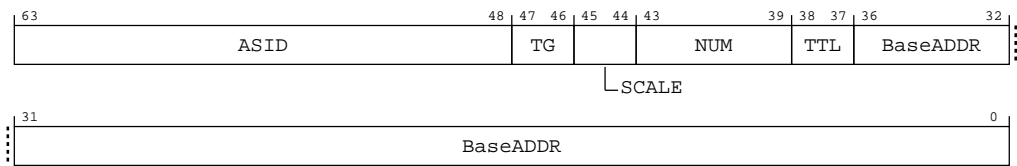
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-219: AARCH64\_TLBI\_RVAE1IS bit assignments



**Table A-585: TLBI RVAE1IS bit descriptions**

Bits	Name	Description	Reset
[63:48]	ASID	<p>ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.</p> <p>Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.</p> <p>If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.</p>	16 {x}
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAE1IS{, &lt;Xt&gt;}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0010	0b001

## Accessibility

TLBI RVAE1IS{, &lt;Xt&gt;}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.20 TLBI RVAE1IS, TLB Range Invalidate by VA, All ASID, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-220: AARCH64\_TLBI\_RVAAE1IS bit assignments

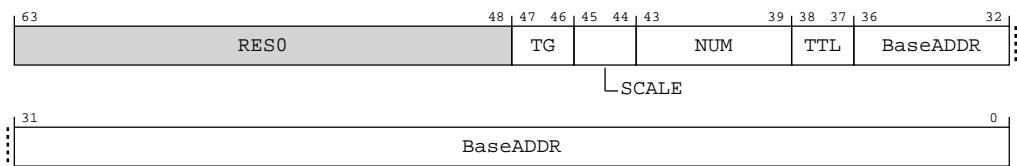


Table A-587: TLBI RVAAE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAAE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0010	0b011

## Accessibility

TLBI RVAAE1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.21 TLBI RVAE1IS, TLB Range Invalidate by VA, Last level, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 \cdot SCALE + 1) \cdot Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $TTL=01$  and  $BaseADDR[29:12]$  is not equal to  $00000000000000000000$ .



- If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-221: AARCH64\_TLBI\_RVALE1IS bit assignments

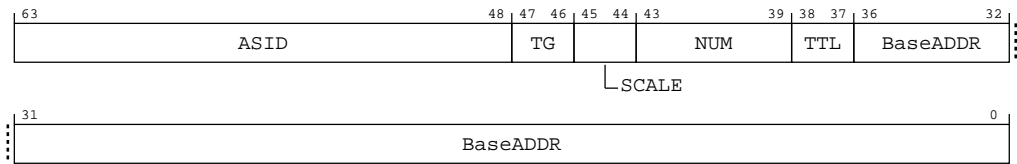


Table A-589: TLBI RVALE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVALE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0010	0b101

## Accessibility

TLBI RVALE1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_ISH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
            TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.22 TLBI RVALE1IS, TLB Range Invalidate by VA, All ASID, Last Level, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry is within the address range determined by the formula  $[BaseADDR (5 \times SCALE + 1) \times Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.

- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 00000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-222: AARCH64\_TLBI\_RVAALE1IS bit assignments

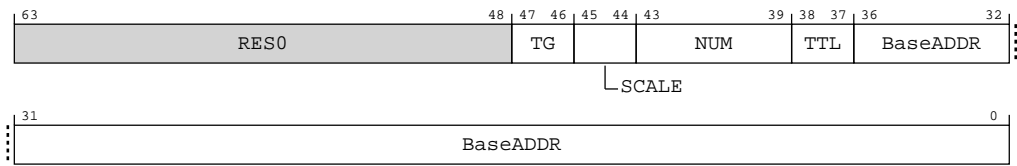


Table A-591: TLBI RVAALE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVAALE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0010	0b111

## Accessibility

TLBI RVAALE1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_ISH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
            TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.23 TLBI VMALLE1IS, TLB Invalidate by VMID, All at stage 1, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

---

From Armv8.4, when



Note

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

---

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

## Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b000

### Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is CONSTRAINED UNPREDICTABLE, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBI_AllAttr);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
    Shareability_ISH, TLBI_AllAttr);
```

#### A.2.4.24 TLBI VAE1IS, TLB Invalidate by VA, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

---

From Armv8.4, when



**Note**

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-223: AARCH64\_TLBI\_VAE1IS bit assignments

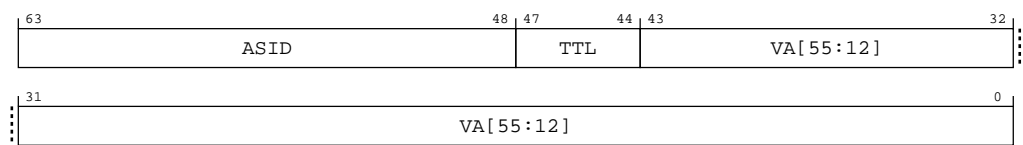


Table A-594: TLBI VAE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}



Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b001

Accessibility

TLBI VAE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
            TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.25 TLBI ASIDE1IS, TLB Invalidate by ASID, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used for the specified ASID, and either:
  - Is from a level of lookup above the final level.
  - Is a non-global entry from the final level of lookup.

The entry would be used with the current VMID and would be required to translate an address using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-224: AARCH64\_TLBI\_ASIDE1IS bit assignments

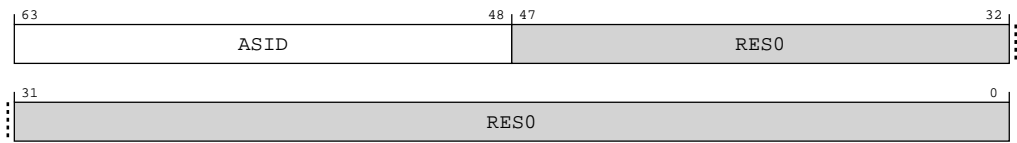


Table A-596: TLBI ASIDE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any appropriate TLB entries that match the ASID values will be affected by this System instruction.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}
[47:0]	RES0	Reserved	RES0

Access

TLBI ASIDE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b010

Accessibility

TLBI ASIDE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_ISH, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
            TLBI_AllAttr, X[t, 64]);
```

A.2.4.26 TLBI VAAE1IS, TLB Invalidate by VA, All ASID, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

From Armv8.4, when



a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.



For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-225: AARCH64\_TLBI\_VAAE1IS bit assignments

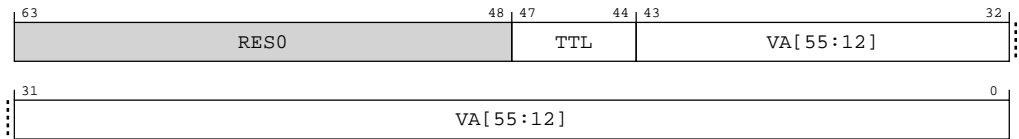


Table A-598: TLBI VAAE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAAE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b011

Accessibility

TLBI VAAE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.27 TLBI VALE1IS, TLB Invalidate by VA, Last level, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

From Armv8.4, when



Note

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-226: AARCH64\_TLBI\_VALE1IS bit assignments

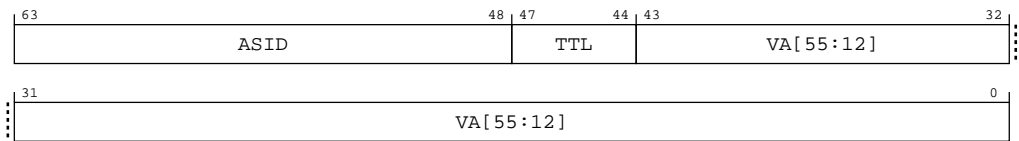


Table A-600: TLBI VALE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}



Access

TLBI VALE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b101

Accessibility

TLBI VALE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
            TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```

A.2.4.28 TLBI VAALE1IS, TLB Invalidate by VA, All ASID, Last Level, EL1, Inner Shareable


Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the final level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.


From Armv8.4, when



Note

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-227: AARCH64\_TLBI\_VAALE1IS bit assignments

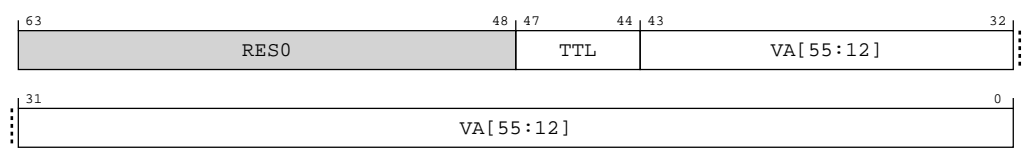


Table A-602: TLBI VAALE1IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

## Access

TLBI VAALE1IS{, &lt;Xt&gt;}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0011	0b111

## Accessibility

TLBI VAALE1IS{, &lt;Xt&gt;}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_ISH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.29 TLBI RVAE1OS, TLB Range Invalidate by VA, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 \times \text{SCALE} + 1) \times \text{Translation\_Granule\_Size}]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 00000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

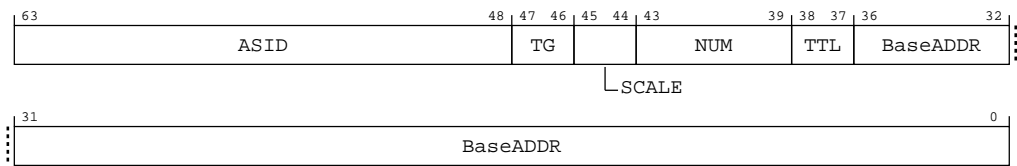
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-228: AARCH64\_TLBI\_RVAE1OS bit assignments



**Table A-604: TLBI RVAE1OS bit descriptions**

Bits	Name	Description	Reset
[63:48]	ASID	<p>ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.</p> <p>Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.</p> <p>If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.</p>	16 {x}
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAE1OS{, &lt;Xt&gt;}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0101	0b001

## Accessibility

TLBI RVAE1OS{, &lt;Xt&gt;}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
    elseif PSTATE.EL == EL2 then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.30 TLBI RVAE1OS, TLB Range Invalidate by VA, All ASID, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-229: AARCH64\_TLBI\_RVAAE1OS bit assignments

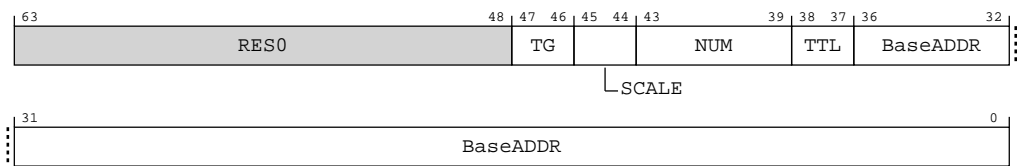


Table A-606: TLBI RVAAE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAAE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0101	0b011

## Accessibility

TLBI RVAAE1OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.31 TLBI RVAE1OS, TLB Range Invalidate by VA, Last level, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 \cdot SCALE + 1) \cdot Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $TTL=01$  and  $BaseADDR[29:12]$  is not equal to  $00000000000000000000$ .

- If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-230: AARCH64\_TLBI\_RVALE1OS bit assignments

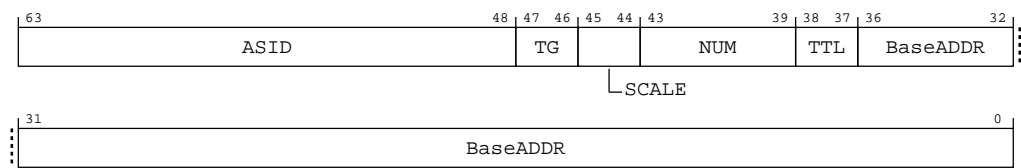


Table A-608: TLBI RVALE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVALE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0101	0b101

## Accessibility

TLBI RVALE1OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.32 TLBI RVALE1OS, TLB Range Invalidate by VA, All ASID, Last Level, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 \times \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

When

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.

- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-231: AARCH64\_TLBI\_RVAALE1OS bit assignments

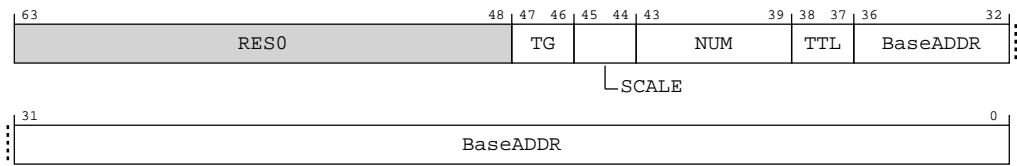


Table A-610: TLBI RVAALE1OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  0b00 Reserved.  0b01 4K translation granule.  0b10 16K translation granule.  0b11 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVAALE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0101	0b111

## Accessibility

TLBI RVAALE1OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
            Shareability_OSH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_OSH,
            TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.33 TLBI RVAE1, TLB Range Invalidate by VA, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 \times \text{SCALE} + 1) \times \text{Translation\_Granule\_Size}]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions



Bit descriptions

Figure A-232: AARCH64\_TLBI\_RVAE1 bit assignments

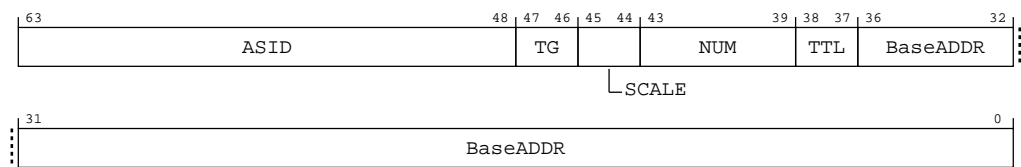


Table A-612: TLBI RVAE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVAE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0110	0b001

## Accessibility

TLBI RVAE1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Any, TLBI_AllAttr, X[t, 64]);

```

#### A.2.4.34 TLBI RVAAE1, TLB Range Invalidate by VA, All ASID, EL1

Invalidate cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 * \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

## Bit descriptions

Figure A-233: AARCH64\_TLBI\_RVAAE1 bit assignments

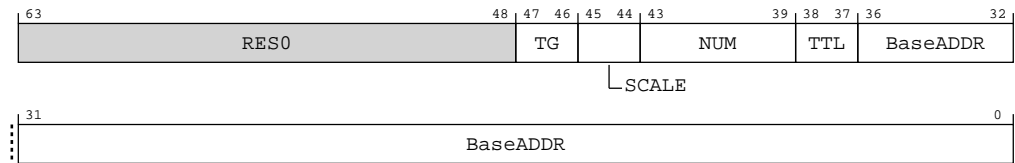


Table A-614: TLBI RVAAE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx

Bits	Name	Description	Reset
[36:0]	BaseADDR	The starting address for the range of the maintenance instruction.  When using a 4KB translation granule, this field is BaseADDR[48:12].  When using a 16KB translation granule, this field is BaseADDR[50:14].  When using a 64KB translation granule, this field is BaseADDR[52:16].	37{x}

## Access

TLBI RVAAE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0110	0b011

## Accessibility

TLBI RVAAE1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FB == '1' then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    elsif PSTATE.EL == EL2 then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
        TLBILevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.35 TLBI RVALE1, TLB Range Invalidate by VA, Last level, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any of the VAs in the specified address range, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

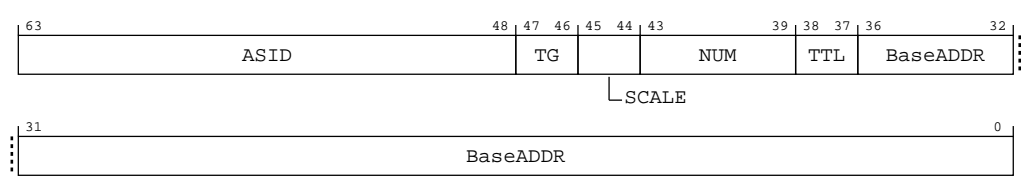
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-234: AARCH64\_TLBI\_RVALE1 bit assignments



**Table A-616: TLBI RVALE1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	ASID	<p>ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.</p> <p>Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.</p> <p>If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.</p>	16 {x}
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVALE1{, &lt;Xt&gt;}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0110	0b101

## Accessibility

TLBI RVALE1{, &lt;Xt&gt;}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.36 TLBI RVALE1, TLB Range Invalidate by VA, All ASID, Last level, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The entry would be used with the current VMID and would be required to translate any of the VAs in the specified address range using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.



- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 00000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-235: AARCH64\_TLBI\_RVAALE1 bit assignments

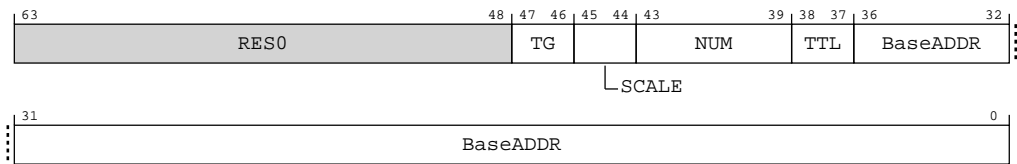


Table A-618: TLBI RVAALE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVAALE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0110	0b111

## Accessibility

TLBI RVAALE1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

A.2.4.37 TLBI VMALLE1, TLB Invalidate by VMID, All at stage 1, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.



For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b000

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
```

```

if HCR_EL2.TTLB == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
elsif HCR_EL2.FB == '1' then
    AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
Shareability_ISH, TLBI_AllAttr);
else
    AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
Shareability_NSH, TLBI_AllAttr);
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_VMALL(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
Shareability_NSH, TLBI_AllAttr);

```

#### A.2.4.38 TLBI VAE1, TLB Invalidate by VA, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is from a level of lookup above the final level and matches the specified ASID.
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

System instructions

##### Access type

See bit descriptions

Bit descriptions

Figure A-236: AARCH64\_TLBI\_VAE1 bit assignments

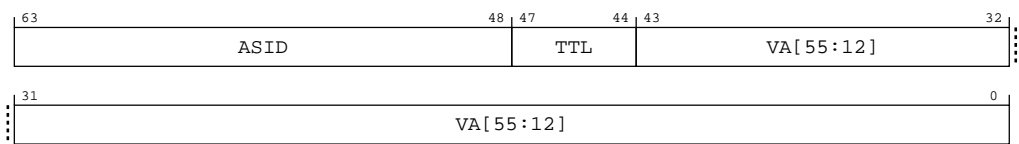


Table A-621: TLBI VAE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b001

Accessibility

TLBI VAE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.39 TLBI ASIDE1, TLB Invalidate by ASID, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used for the specified ASID, and either:
  - Is from a level of lookup above the final level.
  - Is a non-global entry from the final level of lookup.

The entry would be used with the current VMID and would be required to translate an address using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-237: AARCH64\_TLBI\_ASIDE1 bit assignments

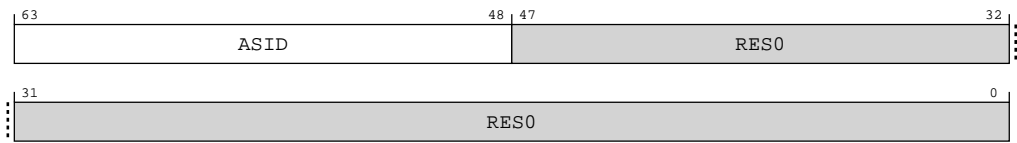


Table A-623: TLBI ASIDE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any appropriate TLB entries that match the ASID values will be affected by this System instruction.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}
[47:0]	RES0	Reserved	RES0

Access

TLBI ASIDE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b010

Accessibility

TLBI ASIDE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ASID(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBI_AllAttr, X[t, 64]);
```



A.2.4.40 TLBI VAAE1, TLB Invalidate by VA, All ASID, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.



For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-238: AARCH64\_TLBI\_VAAE1 bit assignments

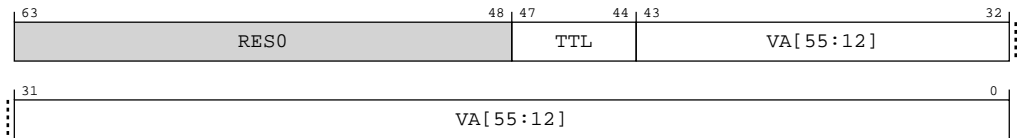


Table A-625: TLBI VAAE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAAE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b011

Accessibility

TLBI VAAE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.41 TLBI VALE1, TLB Invalidate by VA, Last level, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA, and one of the following applies:
  - The entry is a global entry from the final level of lookup.
  - The entry is a non-global entry from the final level of lookup that matches the specified ASID.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&0 translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-239: AARCH64\_TLBI\_VALE1 bit assignments

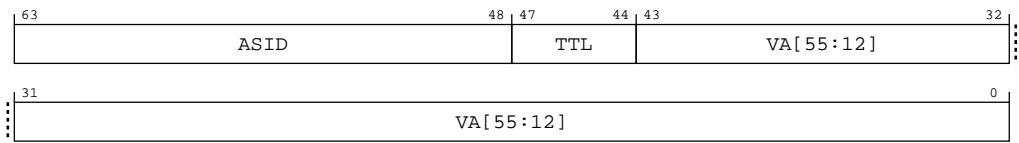


Table A-627: TLBI VALE1 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VALE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b101

Accessibility

TLBI VALE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FB == '1' then
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```


A.2.4.42 TLBI VAALE1, TLB Invalidate by VA, All ASID, Last level, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from the final level of the translation table walk.

The entry would be used with the current VMID and would be required to translate the specified VA using the EL1&O translation regime for the Security state.

The invalidation applies to the PE that executes this System instruction.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

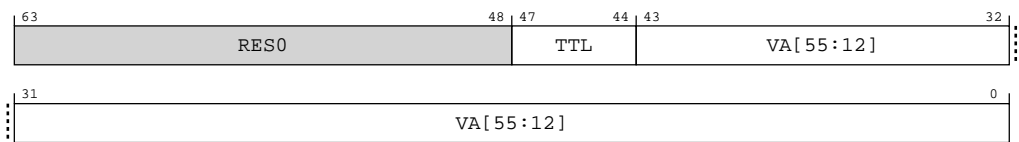
64

**Functional group**  
System instructions

**Access type**  
See bit descriptions

**Bit descriptions**

**Figure A-240: AARCH64\_TLBI\_VAALE1 bit assignments**



**Table A-629: TLBI VAALE1 bit descriptions**

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the VA will be affected by this System instruction, regardless of the ASID.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}



Access

TLBI VAALE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1000	0b0111	0b111

Accessibility

TLBI VAALE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TTLB == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FB == '1' then
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
    else
        AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_VAA(SecurityStateAtEL(EL1), Regime_EL10, VMID[], Shareability_NSH,
    TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```

A.2.4.43 SYS IMP\_BPI, Branch Predictor Invalidation Operation

Invalidates the state of all branch predictors.

Executing this instruction causes all state of the dynamic branch prediction structures (TAGE conditional predictor, CRS, BTAC, nano predictors) to be invalidated, regardless of their context. The invalidation operation takes 128 cycles to execute. In the meantime, any branches encountered on instruction fetches are predicted using static prediction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-241: AARCH64\_SYS\_IMP\_BPI bit assignments

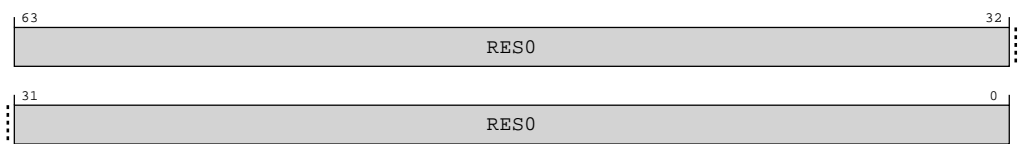


Table A-631: SYS\_IMP\_BPI bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

SYS #0, C15, C1, #1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1111	0b0001	0b001

Accessibility

SYS #0, C15, C1, #1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.BPRED == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_BPI(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_BPI(X[t, 64]);
```

A.2.4.44 SYS\_IMP\_IQBAR, STL Instruction Queue Barrier Operation

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-242: AARCH64\_SYS\_IMP\_IQBAR bit assignments

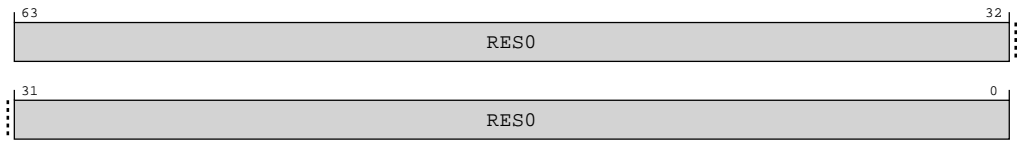


Table A-633: SYS\_IMP\_IQBAR bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the instruction is treated as a **NOP**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

SYS #0, C15, C1, #2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1111	0b0001	0b010

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the instruction is treated as a **NOP**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

SYS #0, C15, C1, #2{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_IQBAR(X[t, 64]);
    elsif PSTATE.EL == EL2 then
```

```
SYS_IMP_IQBAR(X[t, 64]);
```

A.2.4.45 SYS\_IMP\_DFBSTL, STL Data Full Barrier Operation

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-243: AARCH64\_SYS\_IMP\_DFBSTL bit assignments

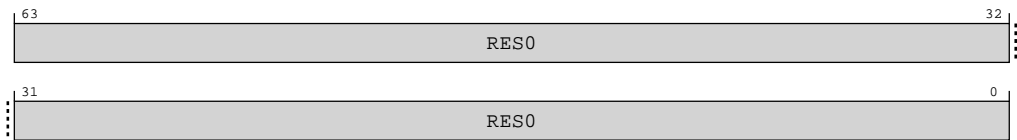


Table A-635: SYS\_IMP\_DFBSTL bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the instruction is treated as a **NOP**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

SYS #0, C15, C1, #3{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b000	0b1111	0b0001	0b011

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the instruction is treated as a NOP.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

SYS #0, C15, C1, #3{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_DFBSTL(X[t, 64]);
elsif PSTATE.EL == EL2 then
    SYS_IMP_DFBSTL(X[t, 64]);
```

A.2.4.46 SYS\_IMP\_CDBGDCT, L1 Data Cache Tag Read Operation

Read contents of the L1 Data Cache Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1 is zeroed.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

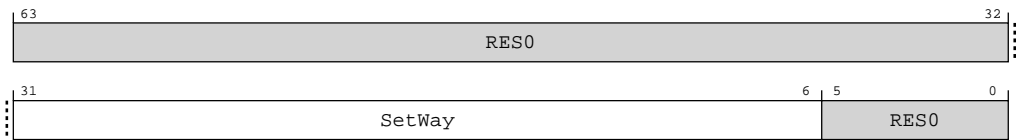
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-244: AARCH64\_SYS\_IMP\_CDBGDCT bit assignments



**Table A-637: SYS\_IMP\_CDBGDCT bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:6]	SetWay	<p>Contains two fields:</p> <ul style="list-style-type: none"> <li>Way, bits[31:30], the number of the way to operate on.</li> <li>Set, bits[S-1:6], the number of the set to operate on.</li> </ul> <p>Bits[29:S] are <b>RES0</b>.</p> <p>The Set width depends on the implemented cache size. The unused bits are <b>RES0</b>. The index is specified as below:</p> <ul style="list-style-type: none"> <li>S=12 for a 16KB cache.</li> <li>S=13 for a 32KB cache.</li> <li>S=14 for a 64KB cache.</li> </ul>	26{x}
[5:0]	<b>RES0</b>	Reserved	<b>RES0</b>

### Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C2, #0{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0010	0b000

### Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C2, #0{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGDCT(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CDBGDCT(X[t, 64]);

```

#### A.2.4.47 SYS\_IMP\_CDBGICT, L1 Instruction Cache Tag Read Operation

Read contents of the L1 Instruction Cache Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1 is zeroed.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-245: AARCH64\_SYS\_IMP\_CDBGICT bit assignments

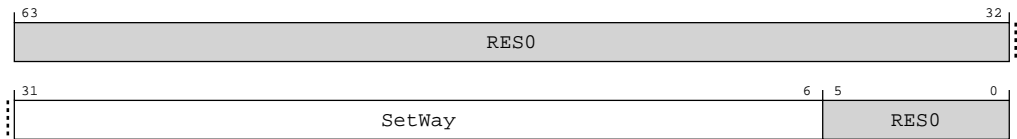


Table A-639: SYS\_IMP\_CDBGICT bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Set, bits[S-1:6], the number of the set to operate on.</li></ul> Bits[29:S] are RES0.  The Set width depends on the implemented cache size. The unused bits are RES0. The index is specified as below: <ul style="list-style-type: none"><li>S=12 for a 16KB cache.</li><li>S=13 for a 32KB cache.</li><li>S=14 for a 64KB cache.</li></ul>	26 {x}
[5:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C2, #1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0010	0b001

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.  
SYS #2, C15, C2, #1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGICT(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CDBGICT(X[t, 64]);
```

A.2.4.48 SYS\_IMP\_CDBGTT, TLB Tag Read Operation

Read contents of the L2 TLB Tag Memory and Walk cache RAM Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1 is zeroed.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-246: AARCH64\_SYS\_IMP\_CDBGTT bit assignments

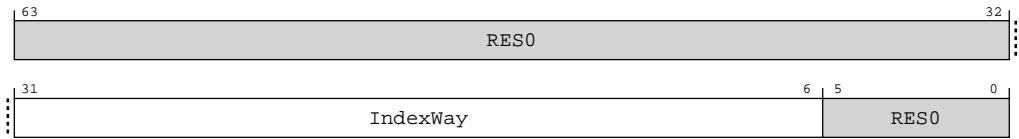


Table A-641: SYS\_IMP\_CDBGTT bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[31:6]	IndexWay	Contains two fields: <ul style="list-style-type: none"> <li>Way, bits[31:30], the number of the way to operate on.</li> <li>Index, bits[14:6], the number of the index to operate on.</li> </ul> Bits[29:15] are <b>RES0</b> .  The index field is used to select the index from the TLB, or walk cache. <ul style="list-style-type: none"> <li>When index is in range 0x000 - 0x0FF, Main TLB is selected.</li> <li>When index is in range 0x100 - 0x107, walk cache is selected.</li> </ul>	26{x}
[5:0]	<b>RES0</b>	Reserved	<b>RES0</b>

### Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C2, #2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0010	0b010

### Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C2, #2{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGTT(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CDBGTT(X[t, 64]);

```

#### A.2.4.49 SYS\_IMP\_CLUSTERCDBGL2T, L2 Cache Tag Read Operation

Read contents of the L2 Cache Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CLUSTERCDBGDRO\_EL1.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-247: AARCH64\_SYS\_IMP\_CLUSTERCDBGL2T bit assignments

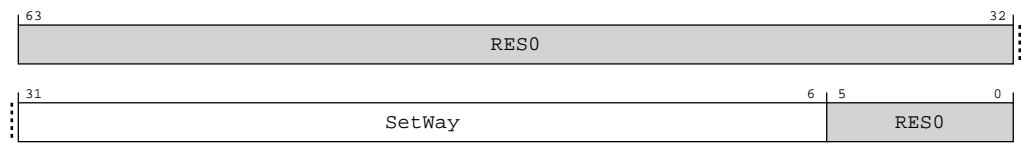



Table A-643: SYS\_IMP\_CLUSTERCDBGL2T bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:29], the number of the way to operate on.</li><li>Set, bits[18:6], the number of the set to operate on.</li></ul> Bits[28:19] are RES0.  <b>Note:</b> The set index width depends on the implemented cache size. The unused bits are RES0.	2 6 { x }
[5:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.



**Note**

If this instruction is executed when the L2 cache size is configured 0, the value returned is 0.

SYS #2, C15, C2, #3{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0010	0b011

## Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.



**Note**

If this instruction is executed when the L2 cache size is configured 0, the value returned is 0.

SYS #2, C15, C2, #3{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CLUSTERCDBGL2T(X[t, 64]);
elsif PSTATE.EL == EL2 then
    SYS_IMP_CLUSTERCDBGL2T(X[t, 64]);

```

### A.2.4.50 SYS\_IMP\_CLUSTERCDBGL2DT, L2 Cache Duplicate L1 Tag Read Operation

Read contents of the L2 Cache Duplicate L1 Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CLUSTERCDBGDRO\_EL1.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions

Bit descriptions

Figure A-248: AARCH64\_SYS\_IMP\_CLUSTERCDBGL2DT bit assignments

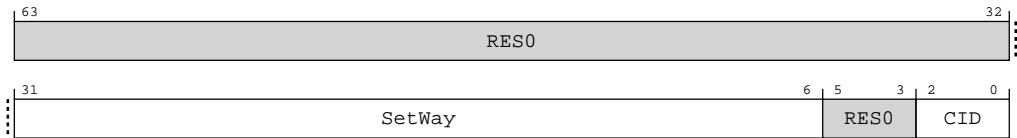


Table A-645: SYS\_IMP\_CLUSTERCDBGL2DT bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Set, bits[13:6], the number of the set to operate on.</li></ul> Bits[29:14] are RES0.  <b>Note:</b> The set index width depends on the implemented cache size. The unused bits are RES0.	26 {x}
[5:3]	RES0	Reserved	RES0
[2:0]	CID	The core ID whose duplicate L1 tags are to be read.	xxx

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

If this instruction is executed with a core number that is larger than the value supported by the implementation, then the instruction performs a read from the duplicate tags of an arbitrary core.

SYS #2, C15, C3, #3{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0011	0b011

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

If this instruction is executed with a core number that is larger than the value supported by the implementation, then the instruction performs a read from the duplicate tags of an arbitrary core.

SYS #2, C15, C3, #3{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
```

```
if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    SYS_IMP_CLUSTERCDBGL2DT(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CLUSTERCDBGL2DT(X[t, 64]);
```

A.2.4.51 SYS\_IMP\_CLUSTERCDBGLCUDT, LCU Duplicate L1 Tag Read Operation

Read contents of the LCU Duplicate L1 Tag Memory.

The 64 bits of cache data returns in AArch64-IMP\_CLUSTERCDBGDRO\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-249: AARCH64\_SYS\_IMP\_CLUSTERCDBGLCUDT bit assignments

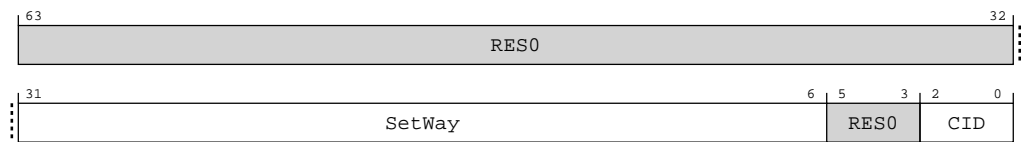


Table A-647: SYS\_IMP\_CLUSTERCDBGLCUDT bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Set, bits[13:6], the number of the set to operate on.</li></ul> Bits[29:14] are RES0.  <b>Note:</b> The set index width depends on the implemented cache size. The unused bits are RES0.	2 {x}
[5:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2:0]	CID	The core ID whose duplicate L1 tags are to be read.	xxx

## Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

If this instruction is executed with a core number that is larger than the value supported by the implementation, then the instruction performs a read from the duplicate tags of an arbitrary core.



If this instruction is executed when the LLRAM is not implemented, the value returned is **UNKNOWN**.

SYS #2, C15, C3, #4{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0011	0b100

## Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

If this instruction is executed with a core number that is larger than the value supported by the implementation, then the instruction performs a read from the duplicate tags of an arbitrary core.



If this instruction is executed when the LLRAM is not implemented, the value returned is **UNKNOWN**.

SYS #2, C15, C3, #4{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CLUSTERCDBGLCU DT(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CLUSTERCDBGLCU DT(X[t, 64]);

```

A.2.4.52 SYS IMP\_CDBGDCD, L1 Data Cache Data Read Operation

Read contents of the L1 Data Cache Data Memory.

The 128 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-250: AARCH64\_SYS\_IMP\_CDBGDCD bit assignments

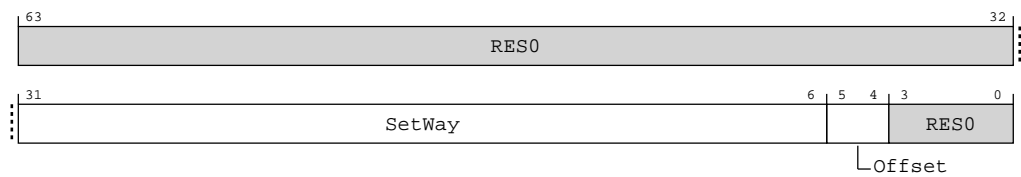


Table A-649: SYS IMP\_CDBGDCD bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Set, bits[S-1:6], the number of the set to operate on.</li></ul> Bits[29:S] are RES0.  The Set width depends on the implemented cache size. The unused bits are RES0. The index is specified as below: <ul style="list-style-type: none"><li>S=12 for a 16KB cache.</li><li>S=13 for a 32KB cache.</li><li>S=14 for a 64KB cache.</li></ul>	26{x}
[5:4]	Offset	Cache data element offset	xx
[3:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C4, #0{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0100	0b000

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C4, #0{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGDCD(X[t, 64]);
elsif PSTATE.EL == EL2 then
    SYS_IMP_CDBGDCD(X[t, 64]);
```

A.2.4.53 SYS\_IMP\_CDBGICD, L1 Instruction Cache Data Read Operation

Read contents of the L1 Instruction Cache Data Memory.

The 128 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions



Bit descriptions

Figure A-251: AARCH64\_SYS\_IMP\_CDBGICD bit assignments

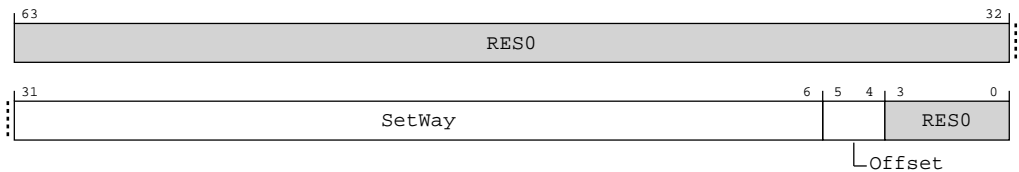


Table A-651: SYS\_IMP\_CDBGICD bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Set, bits[S-1:6], the number of the set to operate on.</li></ul> Bits[29:S] are RES0.  The Set width depends on the implemented cache size. The unused bits are RES0. The index is speficied as below: <ul style="list-style-type: none"><li>S=12 for a 16KB cache.</li><li>S=13 for a 32KB cache.</li><li>S=14 for a 64KB cache.</li></ul>	26 {x}
[5:4]	Offset	Cache data element offset	xx
[3:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

```
SYS #2, C15, C4, #1{, <Xt>}
```

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0100	0b001

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

```
SYS #2, C15, C4, #1{, <Xt>}
```

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGICD(X[t, 64]);
```

```
elseif PSTATE.EL == EL2 then
    SYS_IMP_CDBGICD(X[t, 64]);
```

A.2.4.54 SYS\_IMP\_CDBGTD, TLB Data Read Operation

Read contents of the TLB Data Memory.

The 64 bits of cache data returns in AArch64-IMP\_CDBGDR0\_EL1 and AArch64-IMP\_CDBGDR1\_EL1 is zeroed.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-252: AARCH64\_SYS\_IMP\_CDBGTD bit assignments

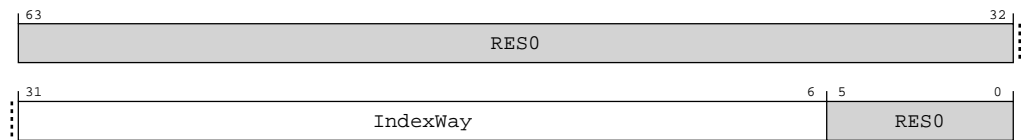


Table A-653: SYS\_IMP\_CDBGTD bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	IndexWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:30], the number of the way to operate on.</li><li>Index, bits[14:6], the number of the index to operate on.</li></ul> Bits[29:15] are RES0.  The index field is used to select the index from the TLB, or walk cache. <ul style="list-style-type: none"><li>When index is in range 0x000 - 0x0FF, Main TLB is selected.</li><li>When index is in range 0x100 - 0x107, walk cache is selected.</li></ul>	26 {x}
[5:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C4, #2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0100	0b010

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.

SYS #2, C15, C4, #2{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CDBGTD(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CDBGTD(X[t, 64]);
```

A.2.4.55 SYS\_IMP\_CLUSTERCDBGL2D, L2 Cache Data Read Operation

Read contents of the L2 Cache Data Memory.

The 64 bits of cache data returns in AArch64-IMP\_CLUSTERCDBGDRO\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-253: AARCH64\_SYS\_IMP\_CLUSTERCDBGL2D bit assignments

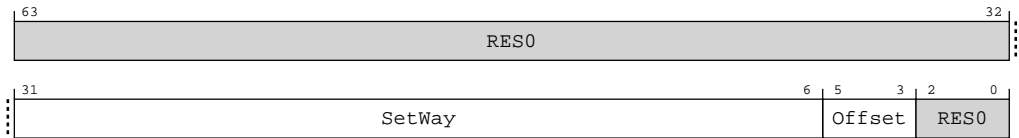


Table A-655: SYS\_IMP\_CLUSTERCDBGL2D bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:6]	SetWay	Contains two fields: <ul style="list-style-type: none"><li>Way, bits[31:29], the number of the way to operate on.</li><li>Set, bits[18:6], the number of the set to operate on.</li></ul> Bits[28:19] are RES0.  <b>Note:</b> The set index width depends on the implemented cache size. The unused bits are RES0.	26 {x}
[5:3]	Offset	Cache data element offset	xxx
[2:0]	RES0	Reserved	RES0

Access

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.



If this instruction is executed when the L2 cache size is configured 0, the value returned is 0.

SYS #2, C15, C4, #3{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b010	0b1111	0b0100	0b011

Accessibility

If this instruction is executed with a set or way argument that is larger than the value supported by the implementation, then the instruction performs a read on a single arbitrary cache line.



If this instruction is executed when the L2 cache size is configured 0, the value returned is 0.

SYS #2, C15, C4, #3{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.CDBG == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        SYS_IMP_CLUSTERCDBGL2D(X[t, 64]);
elseif PSTATE.EL == EL2 then
    SYS_IMP_CLUSTERCDBGL2D(X[t, 64]);
```

#### A.2.4.56 CFP RCTX, Control Flow Prediction Restriction by Context

Control Flow Prediction Restriction by Context applies to all Control Flow Prediction Resources that predict execution based on information gathered within the target execution context or contexts.

Control flow predictions determined by the actions of code in the target execution context or contexts appearing in program order before the instruction cannot exploitatively control speculative execution occurring after the instruction is complete and synchronized.

This instruction is guaranteed to be complete following a DSB that covers both read and write behavior on the same PE as executed the original restriction instruction, and a subsequent context synchronization event is required to ensure that the effect of the completion of the instructions is synchronized to the current execution.



This instruction does not require the invalidation of prediction structures so long as the behavior described for completion of this instruction is met by the implementation.

On some implementations the instruction is likely to take a significant number of cycles to execute. This instruction is expected to be used very rarely, such as on the roll-over of an ASID or VMID, but should not be used on every context switch.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-254: AARCH64\_CFP\_RCTX bit assignments

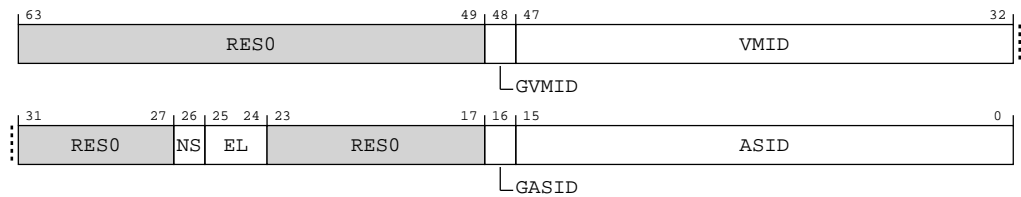


Table A-657: CFP RCTX bit descriptions

Bits	Name	Description	Reset
[63:49]	RES0	Reserved	RES0
[48]	GVMID	Execution of this instruction applies to all VMIDs or a specified VMID.  <b>0b0</b> Applies to specified VMID for an ELO or EL1 target execution context.  <b>0b1</b> Applies to all VMIDs for an ELO or EL1 target execution context.  For target execution contexts other than ELO or EL1, this field is <b>RES0</b> .  If the instruction is executed at ELO or EL1, this field has an Effective value of 0.	x
[47:32]	VMID	Only applies when bit[48] is 0 and the target execution context is either: <ul style="list-style-type: none"><li>EL1.</li><li>EL0.</li></ul> Otherwise this field is <b>RES0</b> .  When the instruction is executed at EL1, this field is treated as the current VMID.  When the instruction is executed at ELO, this field is treated as the current VMID.	16{x}
[31:27]	RES0	Reserved	RES0
[26]	NS	Security State. Defined values are:  <b>0b0</b> Secure state.  <b>0b1</b> Non-secure state.	x

Bits	Name	Description	Reset
[25:24]	EL	Exception Level. Indicates the Exception level of the target execution context.  <b>0b00</b> EL0.  <b>0b01</b> EL1.  <b>0b10</b> EL2.  <b>0b11</b> EL3.  If the instruction is executed at an Exception level lower than the specified level, or is specified to apply to a combination of Exception level and Security state that is not implemented, this instruction is treated as a <b>NOP</b> .	xx
[23:17]	<b>RES0</b>	Reserved	<b>RES0</b>
[16]	GASID	Execution of this instruction applies to all ASIDs or a specified ASID.  <b>0b0</b> Applies to specified ASID for an EL0 target execution context.  <b>0b1</b> Applies to all ASIDs for an EL0 target execution context.  For target execution contexts other than EL0, this field is <b>RES0</b> .  If the instruction is executed at EL0, this field has an Effective value of 0.	x
[15:0]	ASID	Only applies for an EL0 target execution context and when bit[16] is 0.  Otherwise, this field is <b>RES0</b> .  When the instruction is executed at EL0, this field is treated as the current ASID.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being affected only uses 8 bits.	16{x}

## Access

CFP RCTX, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b0011	0b100

## Accessibility

CFP RCTX, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.EnRCTX == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            AArch64.RestrictPrediction(X[t, 64], RestrictType_ControlFlow);
    elseif PSTATE.EL == EL1 then

```

```
AArch64.RestrictPrediction(X[t, 64], RestrictType_ControlFlow);
elseif PSTATE.EL == EL2 then
    AArch64.RestrictPrediction(X[t, 64], RestrictType_ControlFlow);
```

#### A.2.4.57 DVP RCTX, Data Value Prediction Restriction by Context

Data Value Prediction Restriction by Context applies to all Data Value Prediction Resources that predict execution based on information gathered within the target execution context or contexts.



The prediction of the PSTATE.{N,Z,C,V} values is not considered a data value for this purpose.

Data value predictions determined by the actions of code in the target execution context or contexts appearing in program order before the instruction cannot exploitatively control speculative execution occurring after the instruction is complete and synchronized. This instruction is guaranteed to be complete following a DSB that covers both read and write behavior on the same PE as executed the original restriction instruction, and a subsequent context synchronization event is required to ensure that the effect of the completion of the instructions is synchronized to the current execution.



This instruction does not require the invalidation of prediction structures so long as the behavior described for completion of this instruction is met by the implementation. On some implementations the instruction is likely to take a significant number of cycles to execute. This instruction is expected to be used very rarely, such as on the roll-over of an ASID or VMID, but should not be used on every context switch.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions



## Bit descriptions

Figure A-255: AARCH64\_DVP\_RCTX bit assignments

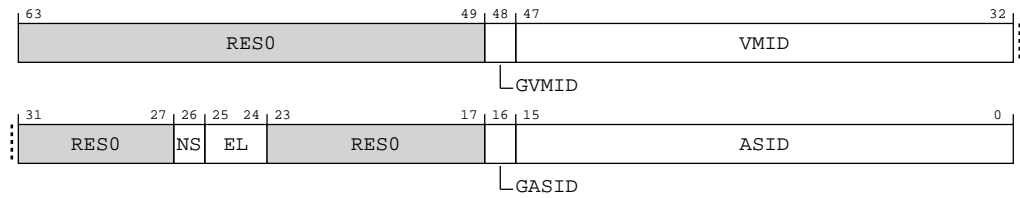


Table A-659: DVP RCTX bit descriptions

Bits	Name	Description	Reset
[63:49]	RES0	Reserved	RES0
[48]	GVMID	<p>Execution of this instruction applies to all VMIDs or a specified VMID.</p> <p><b>0b0</b> Applies to specified VMID for an ELO or EL1 target execution context.</p> <p><b>0b1</b> Applies to all VMIDs for an ELO or EL1 target execution context.</p> <p>For target execution contexts other than ELO or EL1, this field is <b>RES0</b>.</p> <p>If the instruction is executed at ELO or EL1, then this field has an Effective value of 0.</p>	x
[47:32]	VMID	<p>Only applies when bit[48] is 0 and the target execution context is either:</p> <ul style="list-style-type: none"> <li>EL1.</li> <li>ELO.</li> </ul> <p>Otherwise this field is <b>RES0</b>.</p> <p>When the instruction is executed at EL1, this field is treated as the current VMID.</p> <p>When the instruction is executed at ELO, this field is treated as the current VMID.</p>	16{x}
[31:27]	RES0	Reserved	RES0
[26]	NS	<p>Security State. Defined values are:</p> <p><b>0b0</b> Secure state.</p> <p><b>0b1</b> Non-secure state.</p>	x

Bits	Name	Description	Reset
[25:24]	EL	Exception Level. Indicates the Exception level of the target execution context.  <b>0b00</b> EL0.  <b>0b01</b> EL1.  <b>0b10</b> EL2.  <b>0b11</b> EL3.  If the instruction is executed at an Exception level lower than the specified level, or is specified to apply to a combination of Exception level and Security state that is not implemented, this instruction is treated as a <b>NOP</b> .	xx
[23:17]	<b>RES0</b>	Reserved	<b>RES0</b>
[16]	GASID	Execution of this instruction applies to all ASIDs or a specified ASID.  <b>0b0</b> Applies to specified ASID for an EL0 target execution context.  <b>0b1</b> Applies to all ASIDs for an EL0 target execution context.  For target execution contexts other than EL0, this field is <b>RES0</b> .  If the instruction is executed at EL0, this field has an Effective value of 0.	x
[15:0]	ASID	Only applies for an EL0 target execution context and when bit[16] is 0.  Otherwise this field is <b>RES0</b> .  When the instruction is executed at EL0, this field is treated as the current ASID.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being affected only uses 8 bits.	16{x}

## Access

DVP RCTX, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b0011	0b101

## Accessibility

DVP RCTX, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.EnRCTX == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            AArch64.RestrictPrediction(X[t, 64], RestrictType_DataValue);
    elseif PSTATE.EL == EL1 then

```

```
AArch64.RestrictPrediction(X[t, 64], RestrictType_DataValue);
elseif PSTATE.EL == EL2 then
    AArch64.RestrictPrediction(X[t, 64], RestrictType_DataValue);
```

#### A.2.4.58 CPP RCTX, Cache Prefetch Prediction Restriction by Context

Cache Prefetch Prediction Restriction by Context applies to all Cache Allocation Resources that predict cache allocations based on information gathered within the target execution context or contexts.

The actions of code in the target execution context or contexts appearing in program order before the instruction cannot exploitatively control cache prefetch predictions occurring after the instruction is complete and synchronized.

This instruction applies to all:

- Instruction caches.
- Data caches.
- TLB prefetching hardware used by the executing PE that applies to the supplied context or contexts.

This instruction is guaranteed to be complete following a DSB that covers both read and write behavior on the same PE as executed the original restriction instruction, and a subsequent context synchronization event is required to ensure that the effect of the completion of the instructions is synchronized to the current execution.



This instruction does not require the invalidation of Cache Allocation Resources so long as the behavior described for completion of this instruction is met by the implementation.

On some implementations the instruction is likely to take a significant number of cycles to execute. This instruction is expected to be used very rarely, such as on the roll-over of an ASID or VMID, but should not be used on every context switch.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

Bit descriptions

Figure A-256: AARCH64\_CPP\_RCTX bit assignments

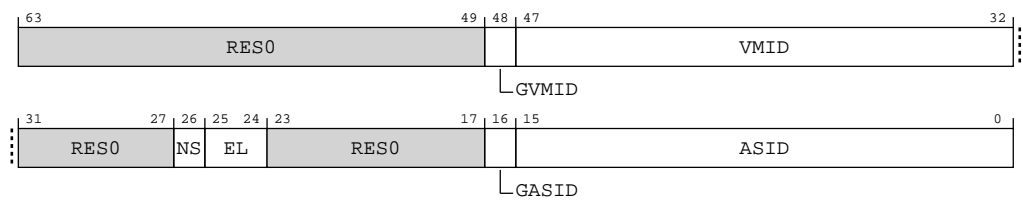


Table A-661: CPP RCTX bit descriptions

Bits	Name	Description	Reset
[63:49]	RES0	Reserved	RES0
[48]	GVMID	Execution of this instruction applies to all VMIDs or a specified VMID. <b>0b0</b> Applies to specified VMID for an ELO or EL1 target execution context. <b>0b1</b> Applies to all VMIDs for an ELO or EL1 target execution context.  For target execution contexts other than ELO and EL1, this field is <b>RES0</b> .  If the instruction is executed at ELO or EL1, this field has an Effective value of 0.	x
[47:32]	VMID	Only applies when bit[48] is 0 and the target execution context is either: <ul style="list-style-type: none"><li>EL1.</li><li>ELO.</li></ul> Otherwise this field is <b>RES0</b> .  When the instruction is executed at EL1, this field is treated as the current VMID.  When the instruction is executed at ELO, this field is treated as the current VMID.	16 {x}
[31:27]	RES0	Reserved	RES0
[26]	NS	Security State. Defined values are: <b>0b0</b> Secure state. <b>0b1</b> Non-secure state.	x

Bits	Name	Description	Reset
[25:24]	EL	Exception Level. Indicates the Exception level of the target execution context.  <b>0b00</b> EL0.  <b>0b01</b> EL1.  <b>0b10</b> EL2.  <b>0b11</b> EL3.  If the instruction is executed at an Exception level lower than the specified level, or is specified to apply to a combination of Exception level and Security state that is not implemented, this instruction is treated as a <b>NOP</b> .	xx
[23:17]	<b>RES0</b>	Reserved	<b>RES0</b>
[16]	GASID	Execution of this instruction applies to all ASIDs or a specified ASID.  <b>0b0</b> Applies to specified ASID for an EL0 target execution context.  <b>0b1</b> Applies to all ASIDs for an EL0 target execution context.  For target execution contexts other than EL0, this field is <b>RES0</b> .  If the instruction is executed at EL0, this field has an Effective value of 0.	x
[15:0]	ASID	Only applies for an EL0 target execution context and when bit[16] is 0.  Otherwise, this field is <b>RES0</b> .  When the instruction is executed at EL0, this field is treated as the current ASID.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being affected only uses 8 bits.	16{x}

## Access

CPP RCTX, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b0011	0b111

## Accessibility

CPP RCTX, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.EnRCTX == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            AArch64.RestrictPrediction(X[t, 64], RestrictType_CachePrefetch);
    elseif PSTATE.EL == EL1 then

```

```
AArch64.RestrictPrediction(X[t, 64], RestrictType_CachePrefetch);
elseif PSTATE.EL == EL2 then
    AArch64.RestrictPrediction(X[t, 64], RestrictType_CachePrefetch);
```

A.2.4.59 DC ZVA, Data Cache Zero by VA

Zero data cache by address. Zeroes a naturally aligned block of N bytes, where the size of N is identified in AArch64-DCZID\_ELO.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-257: AARCH64\_DC\_ZVA bit assignments

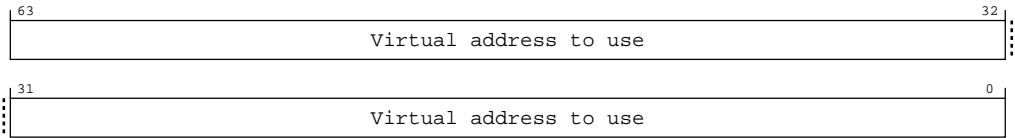


Table A-663: DC ZVA bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. There is no alignment restriction on the address within the block of N bytes that is used.	64 { x }

Access

When this instruction is executed, it can generate memory faults or watchpoints which are prioritized in the same way as other memory-related faults or watchpoints. If a synchronous data abort fault or a watchpoint is generated, the CM bit in the ESR\_ELx.ISS field is set to 0.

If the memory region being zeroed is any type of Device memory, this instruction generates an Alignment fault which is prioritized in the same way as other Alignment faults that are determined by the memory type.

This instruction applies to Normal memory regardless of cacheability attributes.

This instruction behaves as a set of Stores to each byte within the block being accessed, and so it:

- Generates a Permission fault if the translation system does not permit writes to the locations.
- Requires the same considerations for ordering and the management of coherency as any other store instructions.

DC ZVA, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b0100	0b001

### Accessibility

When this instruction is executed, it can generate memory faults or watchpoints which are prioritized in the same way as other memory-related faults or watchpoints. If a synchronous data abort fault or a watchpoint is generated, the CM bit in the ESR\_ELx.ISS field is set to 0.

If the memory region being zeroed is any type of Device memory, this instruction generates an Alignment fault which is prioritized in the same way as other Alignment faults that are determined by the memory type.

This instruction applies to Normal memory regardless of cacheability attributes.

This instruction behaves as a set of Stores to each byte within the block being accessed, and so it:

- Generates a Permission fault if the translation system does not permit writes to the locations.
- Requires the same considerations for ordering and the management of coherency as any other store instructions.

DC ZVA, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTLRL_EL1.DZE == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TDZ == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.MemZero(X[t, 64], CacheType_Data);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TDZ == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.MemZero(X[t, 64], CacheType_Data);
    elsif PSTATE.EL == EL2 then
        AArch64.MemZero(X[t, 64], CacheType_Data);

```

### A.2.4.60 IC IVAU, Instruction Cache line Invalidate by VA to PoU

Invalidate instruction cache by address to Point of Unification.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-258: AARCH64\_IC\_IVAU bit assignments

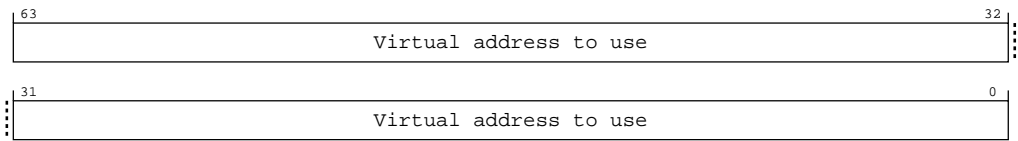


Table A-665: IC IVAU bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Virtual address to use. No alignment restrictions apply to this VA.	64 {x}

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

IC IVAU{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b0101	0b001

Accessibility

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
IC IVAU{, <Xt>}

```
if PSTATE.EL == EL0 then
    if SCTLR_EL1.UCI == '0' then
```



```
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPU == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.IC(X[t, 64], CacheOpScope_PoU);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPU == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.IC(X[t, 64], CacheOpScope_PoU);
    elsif PSTATE.EL == EL2 then
        AArch64.IC(X[t, 64], CacheOpScope_PoU);
```

A.2.4.61 DC CVAC, Data or unified Cache line Clean by VA to PoC

Clean data cache by address to Point of Coherency.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-259: AARCH64\_DC\_CVAC bit assignments

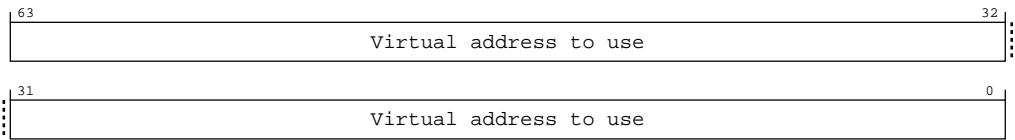


Table A-667: DC CVAC bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 { x }

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC CVAC, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b1010	0b001

### Accessibility

If ELO access is enabled, when executed at EL0, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC CVAC, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTLRL_EL1.UCI == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoC);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoC);
    elsif PSTATE.EL == EL2 then
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoC);

```

### A.2.4.62 DC CVAU, Data or unified Cache line Clean by VA to PoU

Clean data cache by address to Point of Unification.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

Bit descriptions

Figure A-260: AARCH64\_DC\_CVAU bit assignments

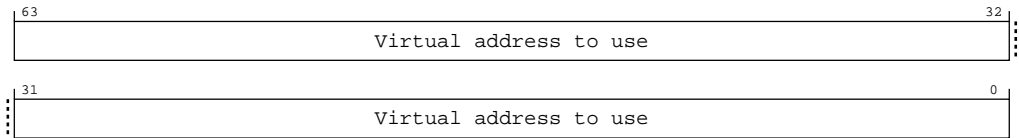


Table A-669: DC CVAU bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 { x }

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC CVAU, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b1011	0b001

Accessibility

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC CVAU, <Xt>

```
if PSTATE.EL == EL0 then
    if SCTLR_EL1.UCI == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPU == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoU);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPU == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoU);
    elsif PSTATE.EL == EL2 then
```

```
AArch64.DC (X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoU);
```

A.2.4.63 DC CVAP, Data or unified Cache line Clean by VA to PoP

Clean data cache by address to Point of Persistence.

If the memory system does not identify a Point of Persistence, then this instruction behaves as a DC CVAC.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-261: AARCH64\_DC\_CVAP bit assignments

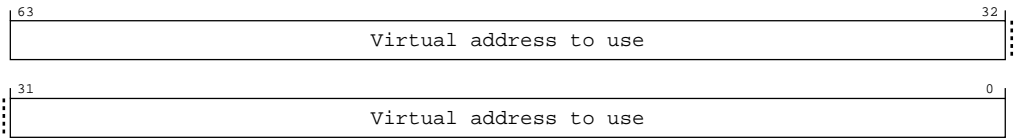


Table A-671: DC CVAP bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 {x}

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC CVAP, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b1100	0b001

### Accessibility

If ELO access is enabled, when executed at EL0, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC CVAP, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.UCI == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoP);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoP);
    elsif PSTATE.EL == EL2 then
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoP);

```

#### A.2.4.64 DC CVADP, Data or unified Cache line Clean by VA to PoDP

Clean data cache by address to Point of Deep Persistence.

If the memory system does not identify a Point of Deep Persistence, then this instruction behaves as a DC CVAP.

### Configurations

This register is present only when IsFeatureImplemented(FEAT\_DPB2). Otherwise, direct accesses to DC CVADP are UNDEFINED.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

Bit descriptions

Figure A-262: AARCH64\_DC\_CVADP bit assignments

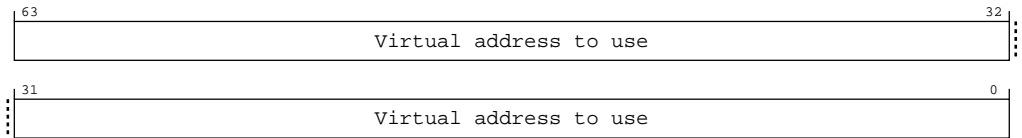


Table A-673: DC CVADP bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 { x }

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC CVADP, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b1101	0b001

Accessibility

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC CVADP, <Xt>

```
if PSTATE.EL == EL0 then
    if SCTLR_EL1.UCI == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoDP);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoDP);
    elsif PSTATE.EL == EL2 then
```

```
AArch64.DC (X[t, 64], CacheType_Data, CacheOp_Clean, CacheOpScope_PoDP);
```

A.2.4.65 DC CIVAC, Data or unified Cache line Clean and Invalidate by VA to PoC

Clean and Invalidate data cache by address to Point of Coherency.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-263: AARCH64\_DC\_CIVAC bit assignments

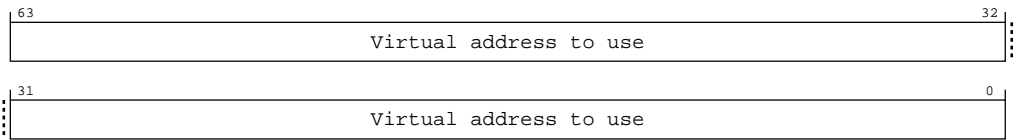


Table A-675: DC CIVAC bit descriptions

Bits	Name	Description	Reset
[63:0]	VA	Virtual address to use. No alignment restrictions apply to this VA.	64 { x }

Access

If ELO access is enabled, when executed at ELO, the instruction may generate a Permission fault, subject to the constraints described in *MMU faults generated by cache maintenance operations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see *The data cache maintenance instruction (DC)* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

DC CIVAC, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b011	0b0111	0b1110	0b001

## Accessibility

If ELO access is enabled, when executed at EL0, the instruction may generate a Permission fault, subject to the constraints described in 'MMU faults generated by cache maintenance operations'.

Execution of this instruction might require an address translation from VA to PA, and that translation might fault. For more information, see 'The data cache maintenance instruction (DC)'.  
DC CIVAC, <Xt>

```

if PSTATE.EL == EL0 then
    if SCTL_EL1.UCI == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_CleanInvalidate,
                CacheOpScope_PoC);
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.TPCP == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.DC(X[t, 64], CacheType_Data, CacheOp_CleanInvalidate,
                CacheOpScope_PoC);
    elsif PSTATE.EL == EL2 then
        AArch64.DC(X[t, 64], CacheType_Data, CacheOp_CleanInvalidate, CacheOpScope_PoC);

```

### A.2.4.66 AT S1E2R, Address Translate Stage 1 EL2 Read

Performs stage 1 address translation as defined for EL2, with permissions as if reading from the given virtual address.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions



Bit descriptions

Figure A-264: AARCH64\_AT\_S1E2R bit assignments

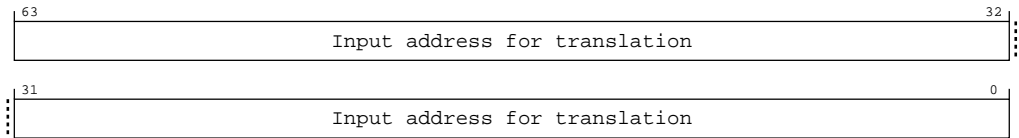


Table A-677: AT S1E2R bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access  
AT S1E2R, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b000

Accessibility  
AT S1E2R, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL2, ATAccess_Read);
```

A.2.4.67 AT S1E2W, Address Translate Stage 1 EL2 Write

Performs stage 1 address translation as defined for EL2, with permissions as if writing to the given virtual address.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-265: AARCH64\_AT\_S1E2W bit assignments

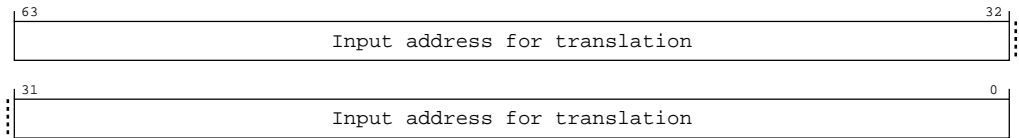


Table A-679: AT S1E2W bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S1E2W, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b001

Accessibility

AT S1E2W, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.AT(X[t, 64], TranslationStage_1, EL2, ATAccess_Write);
```

A.2.4.68 AT S12E1R, Address Translate Stages 1 and 2 EL1 Read

Performs stage 1 and 2 address translation, with permissions as if reading from the given virtual address from EL1, using the EL1&O translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-266: AARCH64\_AT\_S12E1R bit assignments

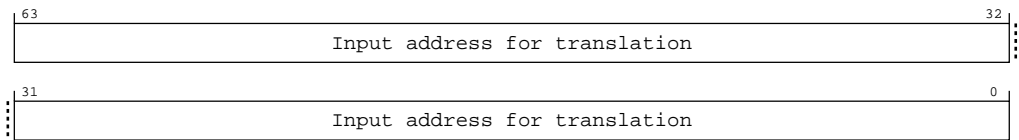


Table A-681: AT S12E1R bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access  
AT S12E1R, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b100

Accessibility  
AT S12E1R, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    if HCR_EL2.<DC,VM> == '00' then
        AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Read);
    else
        AArch64.AT(X[t, 64], TranslationStage_12, EL1, ATAccess_Read);
```

A.2.4.69 AT S12E1W, Address Translate Stages 1 and 2 EL1 Write

Performs stage 1 and 2 address translation, with permissions as if writing to the given virtual address from EL1, using the EL1&O translation regime.

Configurations  
This register is available in all configurations.

Attributes  
Width  
64  
Functional group  
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-267: AARCH64\_AT\_S12E1W bit assignments

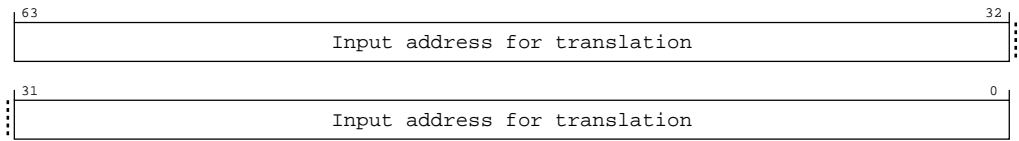


Table A-683: AT S12E1W bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S12E1W, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b101

Accessibility

AT S12E1W, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    if HCR_EL2.<DC,VM> == '00' then
        AArch64.AT(X[t, 64], TranslationStage_1, EL1, ATAccess_Write);
    else
        AArch64.AT(X[t, 64], TranslationStage_12, EL1, ATAccess_Write);
```

A.2.4.70 AT S12E0R, Address Translate Stages 1 and 2 ELO Read

Performs stage 1 and 2 address translations from ELO, with permissions as if reading from the given virtual address from ELO, using the EL1&0 translation regime.

Configurations

This register is available in all configurations.

Attributes

Width

64

**Functional group**  
System instructions

**Access type**  
See bit descriptions

Bit descriptions

Figure A-268: AARCH64\_AT\_S12EOR bit assignments

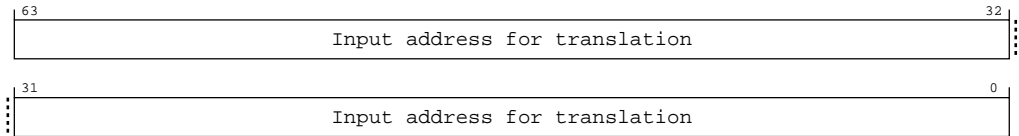


Table A-685: AT S12EOR bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

**Access**  
AT S12EOR, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b110

**Accessibility**  
AT S12EOR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    if HCR_EL2.<DC,VM> == '00' then
        AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Read);
    else
        AArch64.AT(X[t, 64], TranslationStage_12, EL0, ATAccess_Read);
```

A.2.4.71 AT S12EOW, Address Translate Stages 1 and 2 ELO Write

Performs stage 1 and 2 address translations from ELO, with permissions as if writing to the given virtual address from ELO, using the EL1&0 translation regime.

**Configurations**  
This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-269: AARCH64\_AT\_S12E0W bit assignments

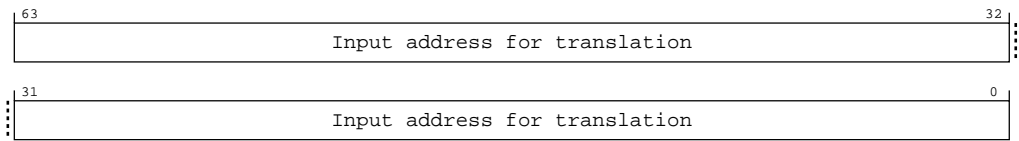


Table A-687: AT S12E0W bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Input address for translation. The resulting address can be read from the AArch64-PAR_EL1.	64 {x}

Access

AT S12E0W, <Xt>

op0	op1	CRn	CRm	op2
0b01	0b100	0b0111	0b1000	0b111

Accessibility

AT S12E0W, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    if HCR_EL2.<DC,VM> == '00' then
        AArch64.AT(X[t, 64], TranslationStage_1, EL0, ATAccess_Write);
    else
        AArch64.AT(X[t, 64], TranslationStage_12, EL0, ATAccess_Write);
```

A.2.4.72 TLBI IPAS2E1IS, TLB Invalidate by Intermediate Physical Address, Stage 2, EL1, Inner Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

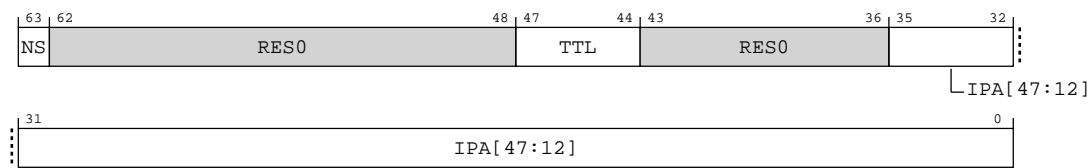
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-270: AARCH64\_TLBI\_IPAS2E1IS bit assignments



**Table A-689: TLBI IPAS2E1IS bit descriptions**

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:44]	TTL	Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.  <b>00xx</b> No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL<1:0> is <b>RES0</b> .  <b>01xx</b> The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Level 1.  0b10 : Level 2.  0b11 : Level 3.  <b>10xx</b> The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Reserved. Treat as if TTL<3:2> is 0b00.  0b10 : Level 2.  0b11 : Level 3.  <b>11xx</b> The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Level 1.  0b10 : Level 2.  0b11 : Level 3.  If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.	xxxx
[43:36]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36 {x}

### Access

TLBI IPAS2E1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0000	0b001

### Accessibility

TLBI IPAS2E1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);

```

#### A.2.4.73 TLBI RIPAS2E1IS, TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1, Inner Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.

- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-271: AARCH64\_TLBI\_RIPAS2E1IS bit assignments

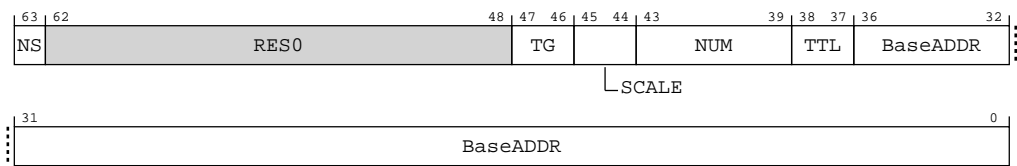


Table A-691: TLBI RIPAS2E1IS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RIPAS2E1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0000	0b010

## Accessibility

TLBI RIPAS2E1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.74 TLBI IPAS2LE1IS, TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Inner Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the final level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions

Bit descriptions

Figure A-272: AARCH64\_TLBI\_IPAS2LE1IS bit assignments

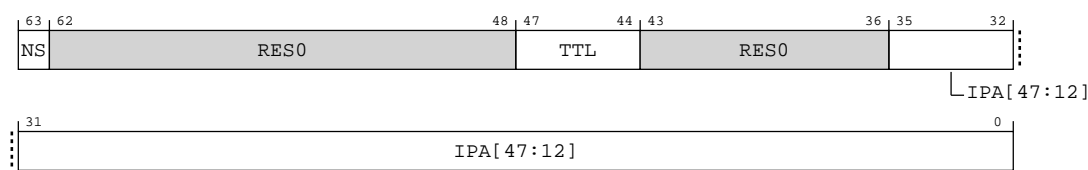


Table A-693: TLBI IPAS2LE1IS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:36]	<b>RES0</b>	Reserved	<b>RES0</b>
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36 {x}

## Access

TLBI IPAS2LE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0000	0b101

## Accessibility

TLBI IPAS2LE1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.75 TLBI IPAS2LE1IS, TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Inner Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-273: AARCH64\_TLBI\_RIPAS2LE1IS bit assignments

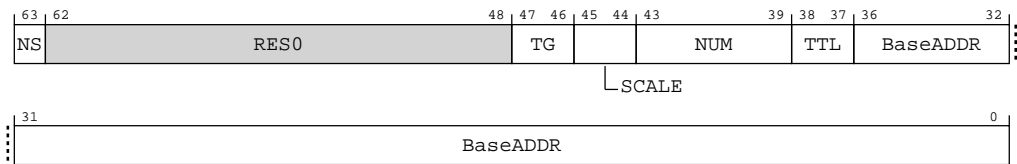


Table A-695: TLBI RIPAS2LE1IS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 { x }



Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RIPAS2LE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0000	0b110

## Accessibility

TLBI RIPAS2LE1IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.76 TLBI ALLE2OS, TLB Invalidate All, EL2, Outer Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

- The entry would be required to translate any address using the EL2&O or EL2 translation regime.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0001	0b000

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL2), Regime_EL2, Shareability_OSH,
        TLBI_AllAttr);
```

A.2.4.77 TLBI VAE2OS, TLB Invalidate by VA, EL2, Outer Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.

- The entry would be required to translate the specified VA using the EL2 translation regime for the Security state.
- The entry is from any level of the translation table walk.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-274: AARCH64\_TLBI\_VAE2OS bit assignments

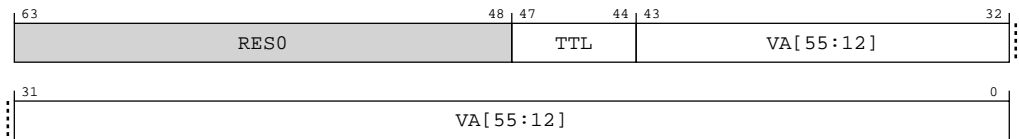


Table A-698: TLBI VAE2OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE2OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0001	0b001

Accessibility

TLBI VAE2OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_OSH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
```


A.2.4.78 TLBI ALLE1OS, TLB Invalidate All, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&O translation regime.

The invalidation applies to entries with any VMID.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0001	0b100

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL1), Regime_EL10, Shareability_OSH,
        TLBI_AllAttr);
```

A.2.4.79 TLBI VALE2OS, TLB Invalidate by VA, Last level, EL2, Outer Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-275: AARCH64\_TLBI\_VALE2OS bit assignments

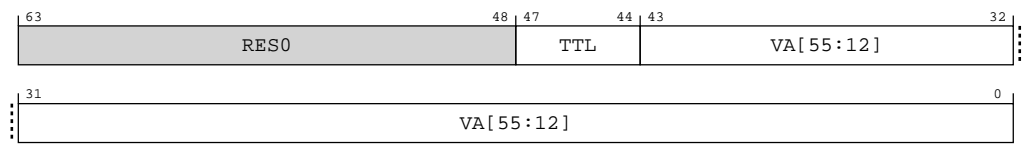


Table A-701: TLBI VALE2OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}



Access

TLBI VALE2OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0001	0b101

Accessibility

TLBI VALE2OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_OSH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
```


A.2.4.80 TLBI VMALLS12E1OS, TLB Invalidate by VMID, All at Stage 1 and 2, EL1, Outer Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&O translation regime.
- The entry would be used with the current VMID.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.


When



Note

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0001	0b110

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI VMALLS12(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBI_AllAttr);
```

A.2.4.81 TLBI RVAE2IS, TLB Range Invalidate by VA, EL2, Inner Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$

using the EL2 translation regime for the Security state.

- The entry is from any level of the translation table walk.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-276: AARCH64\_TLBI\_RVAE2IS bit assignments

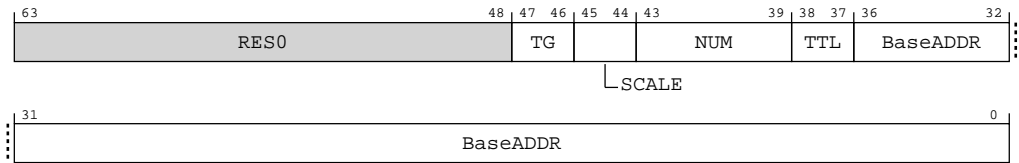


Table A-704: TLBI RVAE2IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAE2IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0010	0b001

## Accessibility

TLBI RVAE2IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_ISH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.82 TLBI RVAE2IS, TLB Range Invalidate by VA, Last level, EL2, Inner Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[\text{BaseADDR} (5 \times \text{SCALE} + 1) \times \text{Translation\_Granule\_Size}]$

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 00000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

## Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-277: AARCH64\_TLBI\_RVALE2IS bit assignments

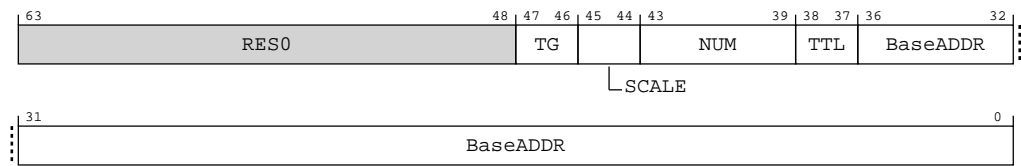


Table A-706: TLBI RVALE2IS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVALE2IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0010	0b101

## Accessibility

TLBI RVALE2IS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_ISH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.83 TLBI ALLE2IS, TLB Invalidate All, EL2, Inner Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.

- The entry would be required to translate any address using the EL2&0 or EL2 translation regime.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0011	0b000

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL2), Regime_EL2, Shareability_ISH,
        TLBI_AllAttr);
```

A.2.4.84 TLBI VAE2IS, TLB Invalidate by VA, EL2, Inner Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.



- The entry would be required to translate the specified VA using the EL2 translation regime for the Security state.
- The entry is from any level of the translation table walk.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-278: AARCH64\_TLBI\_VAE2IS bit assignments

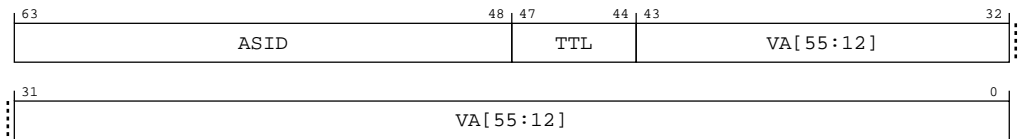


Table A-709: TLBI VAE2IS bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16{x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE2IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0011	0b001

Accessibility

TLBI VAE2IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_ISH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
```


A.2.4.85 TLBI ALLE1IS, TLB Invalidate All, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&O translation regime.

The invalidation applies to entries with any VMID.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0011	0b100

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL1), Regime_EL10, Shareability_ISH,
        TLBI_AllAttr);
```

A.2.4.86 TLBI VALE2IS, TLB Invalidate by VA, Last level, EL2, Inner Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

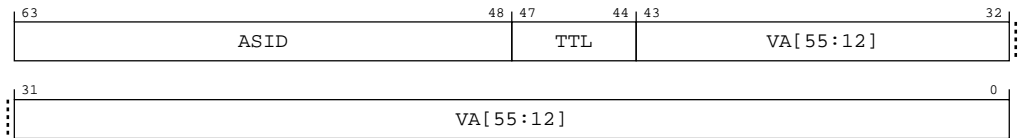
64

**Functional group**  
System instructions

**Access type**  
See bit descriptions

**Bit descriptions**

**Figure A-279: AARCH64\_TLBI\_VALE2IS bit assignments**



**Table A-712: TLBI VALE2IS bit descriptions**

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VALE2IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0011	0b101

Accessibility

TLBI VALE2IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_ISH,
    TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
```


A.2.4.87 TLBI VMALLS12E1IS, TLB Invalidate by VMID, All at Stage 1 and 2, EL1, Inner Shareable

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation applies to all PEs in the same Inner Shareable shareability domain as the PE that executes this System instruction.


From Armv8.4, when



Note

a TLB maintenance instruction is generated to the Secure EL1&0 translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&0 translation of a System MMU in the same required shareability domain with a VMID of 0.



Note

For the EL1&0 translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1IS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0011	0b110

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1IS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI VMALLS12(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_ISH, TLBI_AllAttr);
```

A.2.4.88 TLBI IPAS2E1OS, TLB Invalidate by Intermediate Physical Address, Stage 2, EL1, Outer Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.



The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-280: AARCH64\_TLBI\_IPAS2E1OS bit assignments

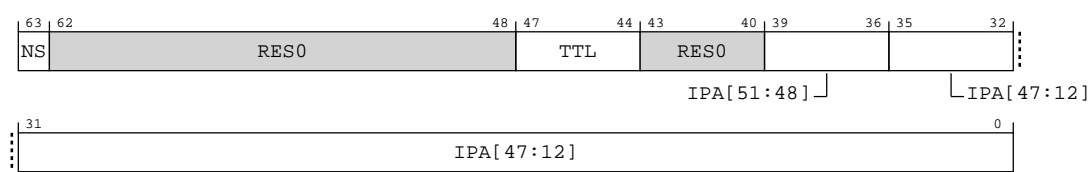


Table A-715: TLBI IPAS2E1OS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:40]	<b>RES0</b>	Reserved	<b>RES0</b>
[39:36]	IPA[51:48]	Extension to IPA[47:12]. For more information, see IPA[47:12].	xxxx
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36{x}

## Access

TLBI IPAS2E1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b000

## Accessibility

TLBI IPAS2E1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
```

### A.2.4.89 TLBI IPAS2E1, TLB Invalidate by Intermediate Physical Address, Stage 2, EL1

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions

Bit descriptions

Figure A-281: AARCH64\_TLBI\_IPAS2E1 bit assignments

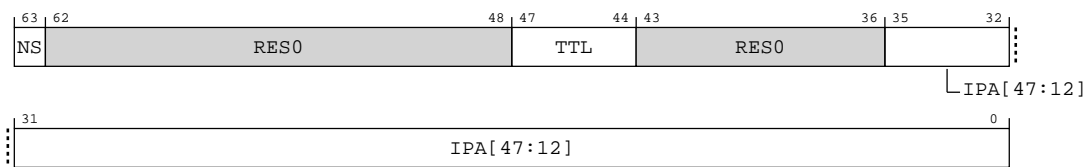


Table A-717: TLBI IPAS2E1 bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:36]	<b>RES0</b>	Reserved	<b>RES0</b>
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36 {x}

## Access

TLBI IPAS2E1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b001

## Accessibility

TLBI IPAS2E1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.90 TLBI RIPAS2E1, TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-282: AARCH64\_TLBI\_RIPAS2E1 bit assignments

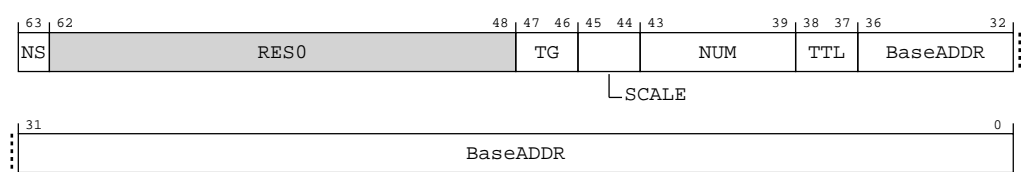


Table A-719: TLBI RIPAS2E1 bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 { x }

Bits	Name	Description	Reset
[38:37]	TTL	<div>TTL Level hint. The TTL hint is only guaranteed to invalidate:<ul style="list-style-type: none"><li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li><li>Leaf-level entries in the range that match the level described by the TTL hint.</li></ul></div> <div><b>0b00</b> The entries in the range can be using any level for the translation table entries.</div> <div><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.  When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</div> <div><b>0b10</b> The TTL hint indicates level 2.</div> <div><b>0b11</b> The TTL hint indicates level 3.</div>	xx
[36:0]	BaseADDR	<div>The starting address for the range of the maintenance instruction.</div> <div>When using a 4KB translation granule, this field is BaseADDR[48:12].</div> <div>When using a 16KB translation granule, this field is BaseADDR[50:14].</div> <div>When using a 64KB translation granule, this field is BaseADDR[52:16].</div>	37{x}

Access

TLBI RIPAS2E1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b010

Accessibility

TLBI RIPAS2E1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```



### A.2.4.91 TLBI RIPAS2E1OS, TLB Range Invalidate by Intermediate Physical Address, Stage 2, EL1, Outer Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 * \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$ .

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-283: AARCH64\_TLBI\_RIPAS2E1OS bit assignments

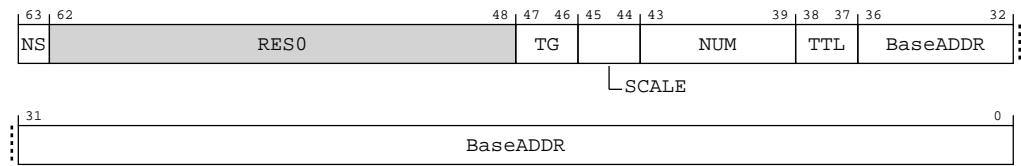


Table A-721: TLBI RIPAS2E1OS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}

Bits	Name	Description	Reset
[38:37]	TTL	<div>TTL Level hint. The TTL hint is only guaranteed to invalidate:<ul style="list-style-type: none"><li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li><li>Leaf-level entries in the range that match the level described by the TTL hint.</li></ul></div> <div><b>0b00</b> The entries in the range can be using any level for the translation table entries.</div> <div><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.  When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</div> <div><b>0b10</b> The TTL hint indicates level 2.</div> <div><b>0b11</b> The TTL hint indicates level 3.</div>	xx
[36:0]	BaseADDR	<div>The starting address for the range of the maintenance instruction.</div> <div>When using a 4KB translation granule, this field is BaseADDR[48:12].</div> <div>When using a 16KB translation granule, this field is BaseADDR[50:14].</div> <div>When using a 64KB translation granule, this field is BaseADDR[52:16].</div>	37{x}

Access

TLBI RIPAS2E1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b011

Accessibility

TLBI RIPAS2E1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBILevel_Any, TLBI_AllAttr, X[t, 64]);
```

A.2.4.92 TLBI IPAS2LE1OS, TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Outer Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the final level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

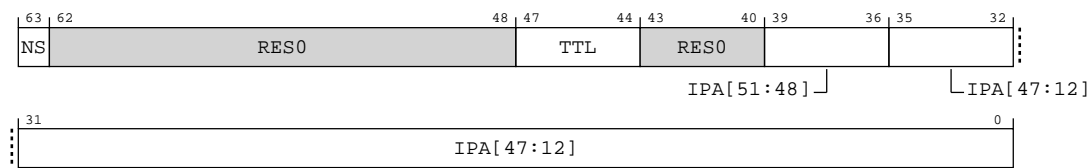
System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-284: AARCH64\_TLBI\_IPAS2LE1OS bit assignments



**Table A-723: TLBI IPAS2LE1OS bit descriptions**

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:44]	TTL	Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.  <b>00xx</b> No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL<1:0> is <b>RES0</b> .  <b>01xx</b> The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Level 1.  0b10 : Level 2.  0b11 : Level 3.  <b>10xx</b> The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Reserved. Treat as if TTL<3:2> is 0b00.  0b10 : Level 2.  0b11 : Level 3.  <b>11xx</b> The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:  0b00 : Reserved. Treat as if TTL<3:2> is 0b00.  0b01 : Level 1.  0b10 : Level 2.  0b11 : Level 3.  If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.	xxxx
[43:40]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[39:36]	IPA[51:48]	Extension to IPA[47:12]. For more information, see IPA[47:12].	xxxx
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36{x}

## Access

TLBI IPAS2LE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b100

## Accessibility

TLBI IPAS2LE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```

### A.2.4.93 TLBI IPAS2LE1, TLB Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the final level of the translation table walk.
- The entry would be required to translate the specified IPA using the EL1&0 translation regime.
- The entry would be used with the current VMID.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to the PE that executes this System instruction.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-285: AARCH64\_TLBI\_IPAS2LE1 bit assignments

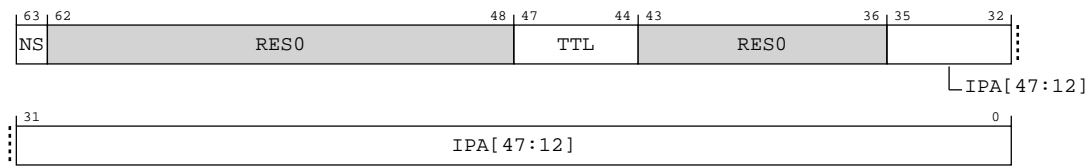


Table A-725: TLBI IPAS2LE1 bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space. <b>0b0</b> IPA is in the Secure IPA space. <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:36]	<b>RES0</b>	Reserved	<b>RES0</b>
[35:0]	IPA[47:12]	Bits[47:12] of the intermediate physical address to match. For implementations with fewer than 48 bits, the upper bits of this field are <b>RES0</b> .	36 {x}

## Access

TLBI IPAS2LE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b101



## Accessibility

TLBI IPAS2LE1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_IPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.94 TLBI RIPAS2LE1, TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$ .

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation only applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If TTL==01 and BaseADDR[29:12] is not equal to 000000000000000000.
  - If TTL==10 and BaseADDR[20:12] is not equal to 0000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-286: AARCH64\_TLBI\_RIPAS2LE1 bit assignments

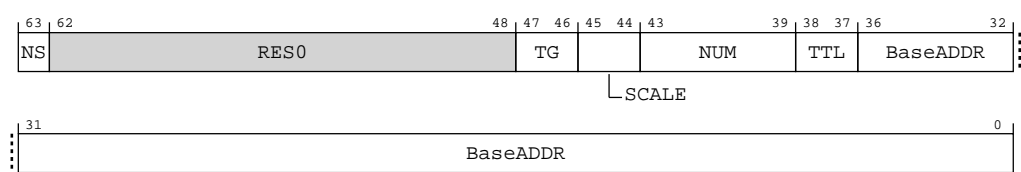


Table A-727: TLBI RIPAS2LE1 bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space.  <b>0b0</b> IPA is in the Secure IPA space.  <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 { x }

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RIPAS2LE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b110

## Accessibility

TLBI RIPAS2LE1{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);

```

#### A.2.4.95 TLBI RIPAS2LE1OS, TLB Range Invalidate by Intermediate Physical Address, Stage 2, Last level, EL1, Outer Shareable

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 2 only translation table entry, from the leaf level of the translation table walk, indicated by the TTL hint.
- The entry would be required to translate any IPA in the specified address range using the EL1&O translation regime.
- The entry would be used with the current VMID.
- The entry is within the address range determined by the formula  $[\text{BaseADDR} (5 * \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$ .

When

a TLB maintenance instruction is generated to the Secure EL1&O translation regime and is defined to pass a VMID argument, then:

- A PE is architecturally required to invalidate all relevant entries in the Secure EL1&O translation of a System MMU in the same required shareability domain with a VMID of 0.

The invalidation is not required to apply to caching structures that combine stage 1 and stage 2 translation table entries.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} = 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} = 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

For more information about the architectural requirements for this System instruction, see *Invalidation of TLB entries from stage 2 translations* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-287: AARCH64\_TLBI\_RIPAS2LE1OS bit assignments

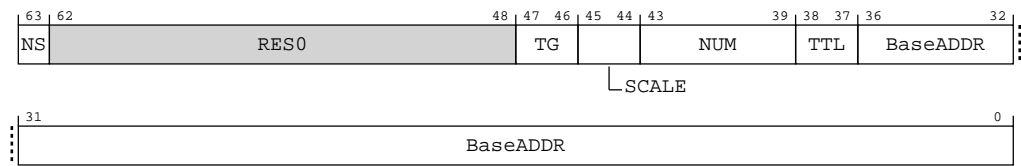


Table A-729: TLBI RIPAS2LE1OS bit descriptions

Bits	Name	Description	Reset
[63]	NS	Not Secure. Specifies the IPA space. <b>0b0</b> IPA is in the Secure IPA space. <b>0b1</b> IPA is in the Non-secure IPA space.	x
[62:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size. <b>0b00</b> Reserved. <b>0b01</b> 4K translation granule. <b>0b10</b> 16K translation granule. <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 { x }

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"><li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li><li>Leaf-level entries in the range that match the level described by the TTL hint.</li></ul> <p><b>0b00</b></p> <p>The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b></p> <p>When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b></p> <p>The TTL hint indicates level 2.</p> <p><b>0b11</b></p> <p>The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

Access

TLBI RIPAS2LE1OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0100	0b111

Accessibility

TLBI RIPAS2LE1OS{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RIPAS2(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_OSH, TLBILevel_Last, TLBI_AllAttr, X[t, 64]);
```

### A.2.4.96 TLBI RVAE2OS, TLB Range Invalidate by VA, EL2, Outer Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[\text{BaseADDR} (5 * \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$

using the EL2 translation regime for the Security state.

- The entry is from any level of the translation table walk.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} = 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} = 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} = 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

### Access type

See bit descriptions

## Bit descriptions

Figure A-288: AARCH64\_TLBI\_RVAE2OS bit assignments

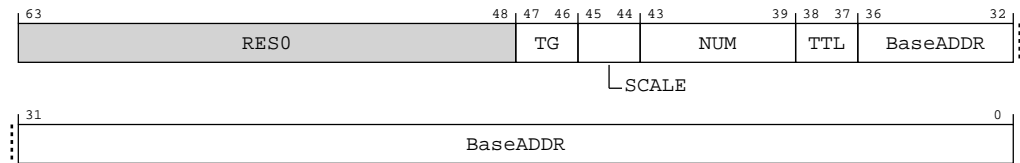


Table A-731: TLBI RVAE2OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx



Bits	Name	Description	Reset
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVAE2OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0101	0b001

## Accessibility

TLBI RVAE2OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_OSH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.97 TLBI RVAE2OS, TLB Range Invalidate by VA, Last level, EL2, Outer Shareable

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[\text{BaseADDR} (5 \times \text{SCALE} + 1) \times \text{Translation\_Granule\_Size}]$

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to all PEs in the same Outer Shareable shareability domain as the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} = 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 0000000000000000.

- If TTL==10 and BaseADDR[20:12] is not equal to 000000000.
- For the 16K translation granule:
  - If TTL==10 and BaseADDR[24:14] is not equal to 000000000000.
- For the 64K translation granule:
  - If TTL==01 and BaseADDR[41:16] is not equal to 00000000000000000000000000000000.
  - If TTL==10 and BaseADDR[28:16] is not equal to 0000000000000000.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-289: AARCH64\_TLBI\_RVALE2OS bit assignments

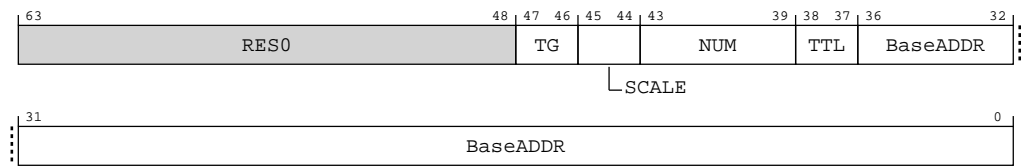


Table A-733: TLBI RVALE2OS bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVALE2OS{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0101	0b101

## Accessibility

TLBI RVALE2OS{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_OSH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.98 TLBI RVAE2, TLB Range Invalidate by VA, EL2

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[\text{BaseADDR} (5 * \text{SCALE} + 1) * \text{Translation\_Granule\_Size}]$

using the EL2 translation regime for the Security state.

- The entry is from any level of the translation table walk.

The invalidation applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[29:12]$  is not equal to 000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $\text{TTL} == 01$  and  $\text{BaseADDR}[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $\text{TTL} == 10$  and  $\text{BaseADDR}[28:16]$  is not equal to 0000000000000000.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-290: AARCH64\_TLBI\_RVAE2 bit assignments

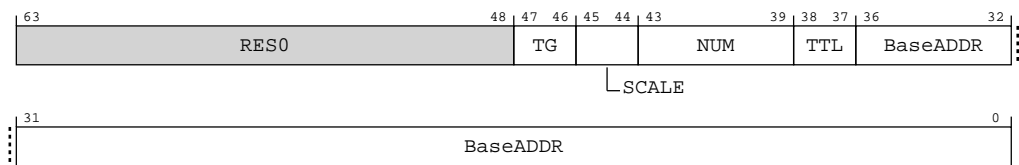


Table A-735: TLBI RVAE2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	Translation granule size.  <b>0b00</b> Reserved.  <b>0b01</b> 4K translation granule.  <b>0b10</b> 16K translation granule.  <b>0b11</b> 64K translation granule.  The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 { x }

Bits	Name	Description	Reset
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37{x}

## Access

TLBI RVAE2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0110	0b001

## Accessibility

TLBI RVAE2{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_NSH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);

```

#### A.2.4.99 TLBI RVALE2, TLB Range Invalidate by VA, Last level, EL2

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk up to the level indicated in the TTL hint.
- The entry would be used to translate any VA

in the range determined by the formula  $[BaseADDR (5 * SCALE + 1) * Translation\_Granule\_Size]$

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to the PE that executes this System instruction.

For translation table entry, the range of addresses invalidated is **UNPREDICTABLE** when:

- For the 4K translation granule:
  - If  $TTL == 01$  and  $BaseADDR[29:12]$  is not equal to 000000000000000000.
  - If  $TTL == 10$  and  $BaseADDR[20:12]$  is not equal to 0000000000.
- For the 16K translation granule:
  - If  $TTL == 10$  and  $BaseADDR[24:14]$  is not equal to 000000000000.
- For the 64K translation granule:
  - If  $TTL == 01$  and  $BaseADDR[41:16]$  is not equal to 00000000000000000000000000000000.
  - If  $TTL == 10$  and  $BaseADDR[28:16]$  is not equal to 0000000000000000.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

System instructions

#### Access type

See bit descriptions

## Bit descriptions

Figure A-291: AARCH64\_TLBI\_RVALE2 bit assignments

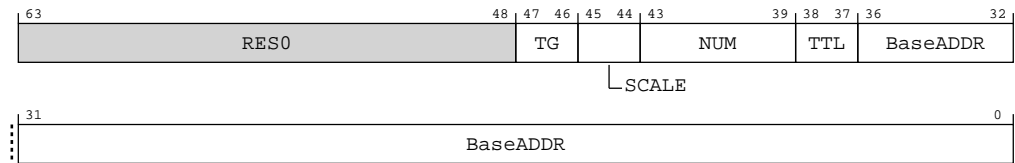


Table A-737: TLBI RVALE2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:46]	TG	<p>Translation granule size.</p> <p><b>0b00</b> Reserved.</p> <p><b>0b01</b> 4K translation granule.</p> <p><b>0b10</b> 16K translation granule.</p> <p><b>0b11</b> 64K translation granule.</p> <p>The instruction takes a translation granule size for the translations that are being invalidated. If the translations used a different translation granule size than the one being specified, then the architecture does not require that the instruction invalidates any entries.</p>	xx
[45:44]	SCALE	The exponent element of the calculation that is used to produce the upper range.	xx
[43:39]	NUM	The base element of the calculation that is used to produce the upper range.	5 {x}
[38:37]	TTL	<p>TTL Level hint. The TTL hint is only guaranteed to invalidate:</p> <ul style="list-style-type: none"> <li>Non-leaf-level entries in the range up to but not including the level described by the TTL hint.</li> <li>Leaf-level entries in the range that match the level described by the TTL hint.</li> </ul> <p><b>0b00</b> The entries in the range can be using any level for the translation table entries.</p> <p><b>0b01</b> When using a 4KB or 64KB translation granule, all entries to invalidate are Level 1 translation table entries.</p> <p>When using a 16KB translation granule, this value is reserved and hardware should treat this field as 0b00.</p> <p><b>0b10</b> The TTL hint indicates level 2.</p> <p><b>0b11</b> The TTL hint indicates level 3.</p>	xx



Bits	Name	Description	Reset
[36:0]	BaseADDR	<p>The starting address for the range of the maintenance instruction.</p> <p>When using a 4KB translation granule, this field is BaseADDR[48:12].</p> <p>When using a 16KB translation granule, this field is BaseADDR[50:14].</p> <p>When using a 64KB translation granule, this field is BaseADDR[52:16].</p>	37 {x}

## Access

TLBI RVALE2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0110	0b101

## Accessibility

TLBI RVALE2{, <Xt>}

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_RVA(SecurityStateAtEL(EL2), Regime_EL2, VMID[], Shareability_NSH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);

```

### A.2.4.100 TLBI ALLE2, TLB Invalidate All, EL2

If EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry, from any level of the translation table walk.
- The entry would be required to translate any address using the EL2&O or EL2 translation regime.

The invalidation only applies to the PE that executes this System instruction.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0111	0b000

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE2{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL2), Regime_EL2, Shareability_NSH,
        TLBI_AllAttr);
```

A.2.4.101 TLBI VAE2, TLB Invalidate by VA, EL2

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be required to translate the specified VA

using the EL2 translation regime for the Security state.

- The entry is from any level of the translation table walk.

The invalidation applies to the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-292: AARCH64\_TLBI\_VAE2 bit assignments

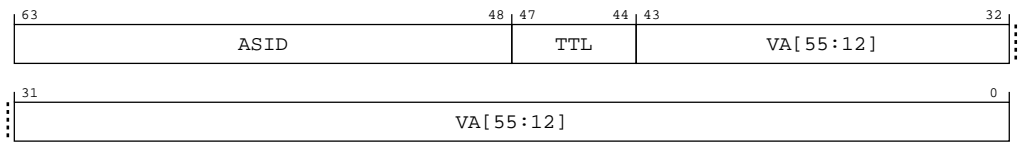


Table A-740: TLBI VAE2 bit descriptions

Bits	Name	Description	Reset
[63:48]	ASID	ASID value to match. Any TLB entries that match the ASID value and VA value will be affected by this System instruction.  Global TLB entries that match the VA value will be affected by this System instruction, regardless of the value of the ASID field.  If the implementation supports 16 bits of ASID, then the upper 8 bits of the ASID must be written to 0 by software when the context being invalidated only uses 8 bits.	16 {x}

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}

Access

TLBI VAE2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0111	0b001

Accessibility

TLBI VAE2{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_NSH,
        TLBIlevel_Any, TLBI_AllAttr, X[t, 64]);
```


A.2.4.102 TLBI ALLE1, TLB Invalidate All, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&O translation regime.

The invalidation applies to entries with any VMID.

The invalidation only applies to the PE that executes this System instruction.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0111	0b100

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI ALLE1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_ALL(SecurityStateAtEL(EL1), Regime_EL10, Shareability_NSH,
        TLBI_AllAttr);
```

A.2.4.103 TLBI VALE2, TLB Invalidate by VA, Last level, EL2

When EL2 is implemented and enabled in the current Security state, invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 translation table entry.
- The entry would be used to translate the specified VA

using the EL2 translation regime for the Security state.

- The entry is from the final level of the translation table walk.

The invalidation applies to the PE that executes this System instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access type

See bit descriptions

Bit descriptions

Figure A-293: AARCH64\_TLBI\_VALE2 bit assignments

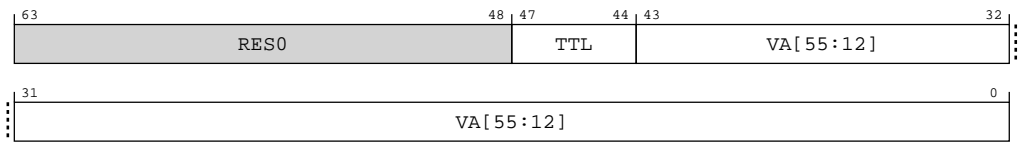


Table A-743: TLBI VALE2 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[47:44]	TTL	<p>Translation Table Level. Indicates the level of the translation table walk that holds the leaf entry for the address being invalidated.</p> <p><b>00xx</b></p> <p>No information supplied as to the translation table level. Hardware must assume that the entry can be from any level. In this case, TTL&lt;1:0&gt; is <b>RES0</b>.</p> <p><b>01xx</b></p> <p>The entry comes from a 4KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>10xx</b></p> <p>The entry comes from a 16KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p><b>11xx</b></p> <p>The entry comes from a 64KB translation granule. The level of walk for the leaf level 0bxx is encoded as:</p> <p>0b00 : Reserved. Treat as if TTL&lt;3:2&gt; is 0b00.</p> <p>0b01 : Level 1.</p> <p>0b10 : Level 2.</p> <p>0b11 : Level 3.</p> <p>If an incorrect value of the TTL field is specified for the entry being invalidated by the instruction, then no entries are required by the architecture to be invalidated from the TLB.</p>	xxxx
[43:0]	VA[55:12]	<p>Bits[55:12] of the virtual address to match. Any appropriate TLB entries that match the ASID value (if appropriate) and VA will be affected by this System instruction.</p> <p>The treatment of the low-order bits of this field depends on the translation granule size, as follows:</p> <ul style="list-style-type: none"> <li>Where a 4KB translation granule is being used, all bits are valid and used for the invalidation.</li> <li>Where a 16KB translation granule is being used, bits [1:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[13:12] have no effect on the operation of the instruction.</li> <li>Where a 64KB translation granule is being used, bits [3:0] of this field are <b>RES0</b> and ignored when the instruction is executed, because VA[15:12] have no effect on the operation of the instruction.</li> </ul>	44 {x}



Access

TLBI VALE2{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0111	0b101

Accessibility

TLBI VALE2{, <Xt>}


```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI_VA(SecurityStateAtEL(EL2), Regime_EL2, VMID_NONE, Shareability_NSH,
        TLBIlevel_Last, TLBI_AllAttr, X[t, 64]);
```

A.2.4.104 TLBI VMALLS12E1, TLB Invalidate by VMID, All at Stage 1 and 2, EL1

Invalidates cached copies of translation table entries from TLBs that meet all the following requirements:

- The entry is a stage 1 or stage 2 translation table entry, from any level of the translation table walk.
- The entry would be required to translate an address using the EL1&O translation regime.
- The entry would be used with the current VMID.

The invalidation applies to the PE that executes this System instruction.



Note

For the EL1&O translation regimes, the invalidation applies to both global entries and non-global entries with any ASID.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

System instructions

Access

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1{, <Xt>}

op0	op1	CRn	CRm	op2
0b01	0b100	0b1000	0b0111	0b110

Accessibility

The Rt field should be set to 0b11111. If the Rt field is not set to 0b11111, it is **CONSTRAINED UNPREDICTABLE**, and the implemented behavior is:

- The instruction behaves as if the Rt field is set to 0b11111.

TLBI VMALLS12E1{, <Xt>}

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    AArch64.TLBI VMALLS12(SecurityStateAtEL(EL1), Regime_EL10, VMID[],
        Shareability_NSH, TLBI_AllAttr);
```

A.2.5 AArch64 Debug register description

This section includes the register descriptions for all Debug registers in the Cortex®-R82AE processor.

A.2.5.1 OSDTRRX\_EL1, OS Lock Data Transfer Register, Receive

Used for save and restore of AArch64-DBGDTRRX\_EL0. It is a component of the Debug Communications Channel.

Configurations

This register is available in all configurations.

Attributes

Width

64

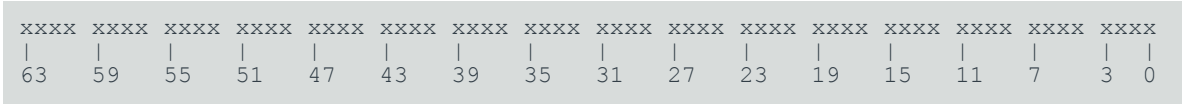
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-294: AARCH64\_OSDTRRX\_EL1 bit assignments

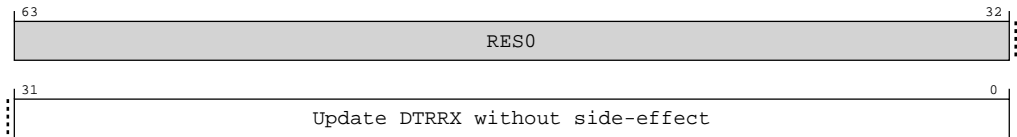


Table A-746: OSDTRRX\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	None	Update DTRRX without side-effect.  Writes to this register update the value in DTRRX and do not change RXfull.  Reads of this register return the last value written to DTRRX and do not change RXfull.  For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	32 {x}

Access

Arm deprecates reads and writes of OSDTRRX\_EL1 when the OS Lock is unlocked.

MRS <Xt>, OSDTRRX\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0000	0b010

MSR OSDTRRX\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0000	0b010

Accessibility

Arm deprecates reads and writes of OSDTRRX\_EL1 when the OS Lock is unlocked.

## MRS &lt;Xt&gt;, OSDTRRX\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif Halted() then
    X[t, 64] = OSDTRRX_EL1;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = OSDTRRX_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = OSDTRRX_EL1;

```

## MSR OSDTRRX\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif Halted() then
    OSDTRRX_EL1 = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        OSDTRRX_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    OSDTRRX_EL1 = X[t, 64];

```

## A.2.5.2 MDCCINT\_EL1, Monitor DCC Interrupt Enable Register

Enables interrupt requests to be signaled based on the DCC status flags.

**Configurations**

This register is available in all configurations.

**Attributes****Width**

64

**Functional group**

Debug registers

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x00x	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-295: AARCH64\_MDCCINT\_EL1 bit assignments

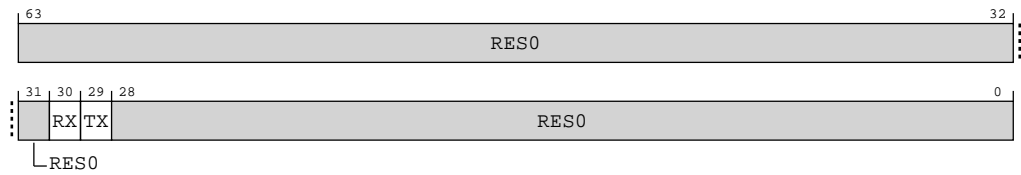


Table A-749: MDCCINT\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0
[30]	RX	DCC interrupt request enable control for DTRRX. Enables a common COMMIRQ interrupt request to be signaled based on the DCC status flags.  <b>0b0</b> No interrupt request generated by DTRRX.  <b>0b1</b> Interrupt request will be generated on RXfull == 1.	0b0
[29]	TX	DCC interrupt request enable control for DTRTX. Enables a common COMMIRQ interrupt request to be signaled based on the DCC status flags.  <b>0b0</b> No interrupt request generated by DTRTX.  <b>0b1</b> Interrupt request will be generated on TXfull == 0.	0b0
[28:0]	RES0	Reserved	RES0

Access

MRS <Xt>, MDCCINT\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0010	0b000

MSR MDCCINT\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0010	0b000

Accessibility

MRS <Xt>, MDCCINT\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif Halted() then
    X[t, 64] = MDCCINT_EL1;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MDCCINT_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = MDCCINT_EL1;
```

MSR MDCCINT\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif Halted() then
    MDCCINT_EL1 = X[t, 64];
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        MDCCINT_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    MDCCINT_EL1 = X[t, 64];
```

A.2.5.3 MDSCR\_EL1, Monitor Debug System Control Register

Main control register for the debug implementation.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Debug registers

Access type

R

Reset value

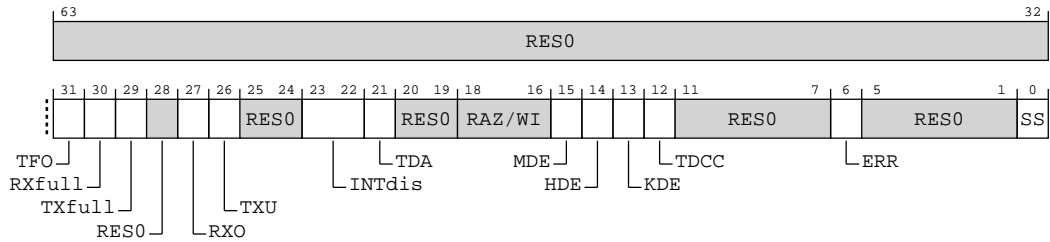
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-296: AARCH64\_MDSCR\_EL1 bit assignments**



**Table A-752: MDSCR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	TFO	Trace Filter override. Used for save/restore of ext-EDSCR.TFO.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.TFO. Reads and writes of this bit are indirect accesses to ext-EDSCR.TFO.  <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW  <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x
[30]	RXfull	Used for save/restore of ext-EDSCR.RXfull.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.RXfull. Reads and writes of this bit are indirect accesses to ext-EDSCR.RXfull.  <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW  <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>21</sup>

<sup>21</sup> The architected behavior of this field determines the value it returns after a reset.

Bits	Name	Description	Reset
[29]	TXfull	Used for save/restore of ext-EDSCR.TXfull.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.TXfull. Reads and writes of this bit are indirect accesses to ext-EDSCR.TXfull. <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>22</sup>
[28]	RES0	Reserved	RES0
[27]	RXO	Used for save/restore of ext-EDSCR.RXO.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.RXO. Reads and writes of this bit are indirect accesses to ext-EDSCR.RXO.  When AArch64-OSLSR_EL1.OSLK == 1, if bits [27,6] of the value written to MDSCR_EL1 are {1,0}, that is, the RXO bit is 1 and the ERR bit is 0, the PE sets ext-EDSCR.{RXO,ERR} to <b>UNKNOWN</b> values. <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>23</sup>
[26]	TXU	Used for save/restore of ext-EDSCR.TXU.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.TXU. Reads and writes of this bit are indirect accesses to ext-EDSCR.TXU.  When AArch64-OSLSR_EL1.OSLK == 1, if bits [26,6] of the value written to MDSCR_EL1 are {1,0}, that is, the TXU bit is 1 and the ERR bit is 0, the PE sets ext-EDSCR.{TXU,ERR} to <b>UNKNOWN</b> values. <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>24</sup>
[25:24]	RES0	Reserved	RES0

<sup>22</sup> The architected behavior of this field determines the value it returns after a reset.<sup>23</sup> The architected behavior of this field determines the value it returns after a reset.<sup>24</sup> The architected behavior of this field determines the value it returns after a reset.



Bits	Name	Description	Reset
[23:22]	INTdis	Used for save/restore of ext-EDSCR.INTdis.  When AArch64-OSLSR_EL1.OSLK == 0, and software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this field holds the value of ext-EDSCR.INTdis. Reads and writes of this field are indirect accesses to ext-EDSCR.INTdis.  <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW  <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	xx <sup>25</sup>
[21]	TDA	Used for save/restore of ext-EDSCR.TDA.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.TDA. Reads and writes of this bit are indirect accesses to ext-EDSCR.TDA.  <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW  <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>26</sup>
[20:19]	RES0	Reserved	RES0
[18:16]	RAZ/WI	Reserved	RAZ/WI
[15]	MDE	Monitor debug events. Enable Breakpoint, Watchpoint, and Vector Catch exceptions.  <b>0b0</b> Breakpoint, Watchpoint, and Vector Catch exceptions disabled.  <b>0b1</b> Breakpoint, Watchpoint, and Vector Catch exceptions enabled.	x
[14]	HDE	Used for save/restore of ext-EDSCR.HDE.  When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.  When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.HDE. Reads and writes of this bit are indirect accesses to ext-EDSCR.HDE.  <b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW  <b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO	x <sup>27</sup>
[13]	KDE	Local (kernel) debug enable. If EL <sub>D</sub> is using AArch64, enable debug exceptions within EL <sub>D</sub> . Permitted values are:  <b>0b0</b> Debug exceptions, other than Breakpoint Instruction exceptions, disabled within EL <sub>D</sub> .  <b>0b1</b> All debug exceptions enabled within EL <sub>D</sub> .	x

<sup>25</sup> The architected behavior of this field determines the value it returns after a reset.<sup>26</sup> The architected behavior of this field determines the value it returns after a reset.<sup>27</sup> The architected behavior of this field determines the value it returns after a reset.

Bits	Name	Description	Reset
[12]	TDCC	<p>Traps EL0 accesses to the Debug Communication Channel (DCC) registers to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, from both Execution states, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, MRS or MSR accesses to the following DCC registers are trapped, reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-MDCCSR_ELO.</li> <li>If not in Debug state, AArch64-DBGDTR_ELO, AArch64-DBGDTRTX_ELO, and AArch64-DBGDTRRX_ELO.</li> </ul> </li> </ul> <p><b>0b0</b> This control does not cause any instructions to be trapped.</p> <p><b>0b1</b> EL0 using AArch64: EL0 accesses to the AArch64 DCC registers are trapped.</p>	x
[11:7]	RES0	Reserved	RES0
[6]	ERR	<p>Used for save/restore of ext-EDSCR.ERR.</p> <p>When AArch64-OSLSR_EL1.OSLK == 0, software must treat this bit as UNK/SBZP.</p> <p>When AArch64-OSLSR_EL1.OSLK == 1, this bit holds the value of ext-EDSCR.ERR. Reads and writes of this bit are indirect accesses to ext-EDSCR.ERR.</p> <p><b>When AArch64-OSLSR_EL1.OSLK == '1'</b> Access to this field is: RW</p> <p><b>When AArch64-OSLSR_EL1.OSLK == '0'</b> Access to this field is: RO</p>	x <sup>28</sup>
[5:1]	RES0	Reserved	RES0
[0]	SS	<p>Software step control bit. If EL<sub>D</sub> is using AArch64, enable Software step. Permitted values are:</p> <p><b>0b0</b> Software step disabled</p> <p><b>0b1</b> Software step enabled.</p>	x

## Access

MRS <Xt>, MDSCR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0010	0b010

MSR MDSCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0010	0b010

<sup>28</sup> The architected behavior of this field determines the value it returns after a reset.

## Accessibility

MRS <Xt>, MDSCR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MDSCR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = MDSCR_EL1;

```

MSR MDSCR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        MDSCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    MDSCR_EL1 = X[t, 64];

```

### A.2.5.4 OSDTRTX\_EL1, OS Lock Data Transfer Register, Transmit

Used for save/restore of AArch64-DBGDTRTX\_EL0. It is a component of the Debug Communications Channel.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Debug registers

### Access type

See bit descriptions

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-297: AARCH64\_OSDTRTX\_EL1 bit assignments

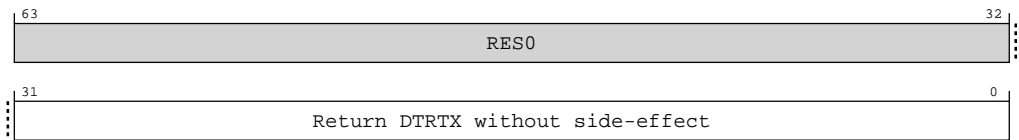


Table A-755: OSDTRTX\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	None	Return DTRTX without side-effect.  Reads of this register return the value in DTRTX and do not change TXfull.  Writes of this register update the value in DTRTX and do not change TXfull.  For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <i>Arm® Architecture Reference Manual for A-profile architecture</i> .	32 {x}

Access

Arm deprecates reads and writes of OSDTRTX\_EL1 when the OS Lock is unlocked.

MRS <Xt>, OSDTRTX\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0011	0b010

MSR OSDTRTX\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0011	0b010

Accessibility

Arm deprecates reads and writes of OSDTRTX\_EL1 when the OS Lock is unlocked.

MRS <Xt>, OSDTRTX\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif Halted() then
    X[t, 64] = OSDTRTX_EL1;
```

```

elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = OSDTRTX_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = OSDTRTX_EL1;

```

MSR OSDTRTX\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif Halted() then
    OSDTRTX_EL1 = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        OSDTRTX_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    OSDTRTX_EL1 = X[t, 64];

```

### A.2.5.5 OSECCR\_EL1, OS Lock Exception Catch Control Register

Provides a mechanism for an operating system to access the contents of ext-EDECCR that are otherwise invisible to software, so it can save/restore the contents of ext-EDECCR over powerdown on behalf of the external debugger.

#### Configurations

If AArch64-OSLSR\_EL1.OSLK == 0, then OSECCR\_EL1 returns an UNKNOWN value on reads and ignores writes.

AArch64 register OSECCR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.9 EDECCR, External Debug Exception Catch Control Register](#) on page 1741 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Debug registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

When AArch64-OSLSR\_EL1.OSLK == '1'

Figure A-298: AARCH64\_OSECCR\_EL1 bit assignments

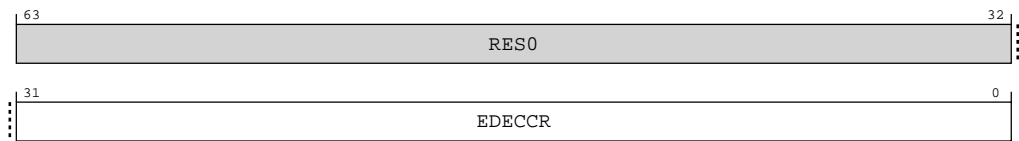


Table A-758: OSECCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	EDECCR	Used for save/restore to ext-EDECCR over powerdown.  Reads or writes to this field are indirect accesses to ext-EDECCR.	32 {x}

Access

MRS <Xt>, OSECCR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0110	0b010

MSR OSECCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	0b0110	0b010

Accessibility

MRS <Xt>, OSECCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif OSLSR_EL1.OSLK == '0' then
        X[t, 64] = bits(64) UNKNOWN;
    else
        X[t, 64] = OSECCR_EL1;
    elsif PSTATE.EL == EL2 then
        if OSLSR_EL1.OSLK == '0' then
            X[t, 64] = bits(64) UNKNOWN;
```

```
else
    X[t, 64] = OSECCR_EL1;
```

MSR OSECCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif OSLSR_EL1.OSLK == '0' then
        return;
    else
        OSECCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' then
        return;
    else
        OSECCR_EL1 = X[t, 64];
```

#### A.2.5.6 DBGBVR<n>\_EL1, Debug Breakpoint Value Registers, n = 0 - 5

Holds a virtual address, or a VMID and/or a context ID, for use in breakpoint matching. Forms breakpoint n together with control register AArch64-DBGBCR<n>\_EL1.

#### Configurations

How this register is interpreted depends on the value of AArch64-DBGBCR<n>\_EL1.BT.

- When AArch64-DBGBCR<n>\_EL1.BT is 0b000x, this register holds a virtual address.
- When AArch64-DBGBCR<n>\_EL1.BT is 0b001x, 0b011x, or 0b110x, this register holds a Context ID.
- When AArch64-DBGBCR<n>\_EL1.BT is 0b100x, this register holds a VMID.
- When AArch64-DBGBCR<n>\_EL1.BT is 0b101x, this register holds a VMID and a Context ID.
- When AArch64-DBGBCR<n>\_EL1.BT is 0b111x, this register holds two Context ID values.

For other values of AArch64-DBGBCR<n>\_EL1.BT, this register is RES0.

If breakpoint n is not implemented then accesses to this register are UNDEFINED.

AArch64 register DBGBVR<n>\_EL1 bits [63:0] are architecturally mapped to External register [B.2.2.1.13 DBGBVR<n>\\_EL1, Debug Breakpoint Value Registers, n = 0 - 5](#) on page 1753 bits [63:0].

#### Attributes

##### Width

64

##### Functional group

Debug registers

Access type

See bit descriptions

Reset value

When AArch64-DBGBCR<n>\_EL1.BT == '000x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '001x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '011x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '100x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '101x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '110x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When AArch64-DBGBCR<n>\_EL1.BT == '111x'

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When AArch64-DBGBCR<n>\_EL1.BT == '000'

Figure A-299: AARCH64\_DBGBCR<n>\_EL1 bit assignments

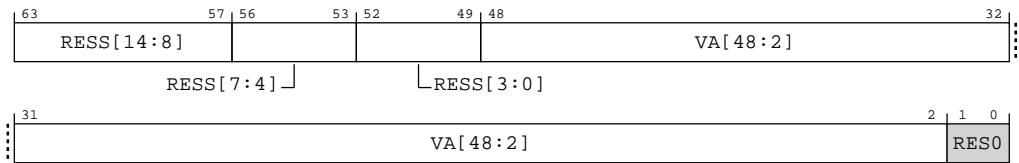


Table A-761: DBGBCR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:57]	RESS[14:8]	Reserved, Sign extended. Software must set all bits in this field to the same value as the most significant bit of the VA field. If all bits in this field are not the same value as the most significant bit of the VA field, then the PE ignores this field when comparing an address, and if the breakpoint is not context-aware, the value read back in each bit of this field is a copy of the most significant bit of the VA field.	7 { x }
[56:53]	RESS[7:4]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx



Bits	Name	Description	Reset
[52:49]	RESS[3:0]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[48:2]	VA[48:2]	Bits[48:2] of the address value for comparison.	47 { x }
[1:0]	RES0	Reserved	RES0

When AArch64-DBGBCR<n>\_EL1.BT == '001'

Figure A-300: AARCH64\_DBGGBVR<n>\_EL1 bit assignments

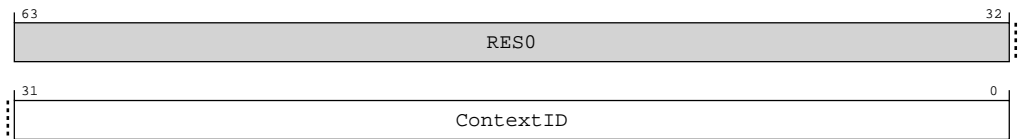


Table A-762: DBGGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	ContextID	Context ID value for comparison.  The value is compared against AArch64-CONTEXTIDR_EL1.	32 { x }

When AArch64-DBGBCR<n>\_EL1.BT == '011'

Figure A-301: AARCH64\_DBGGBVR<n>\_EL1 bit assignments

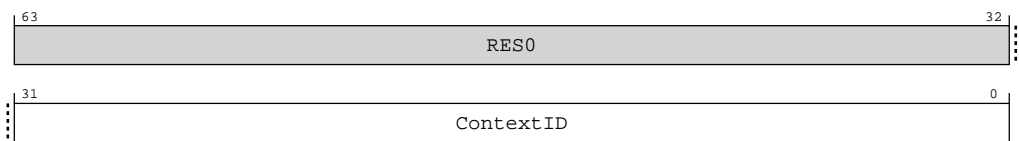
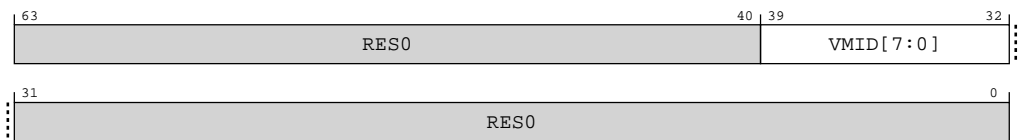


Table A-763: DBGGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32 { x }

When AArch64-DBGBCR<n>\_EL1.BT == '100'

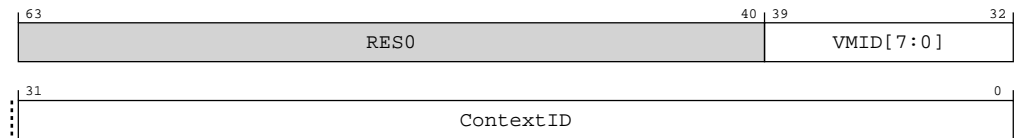
Figure A-302: AARCH64\_DBGGBVR<n>\_EL1 bit assignments



**Table A-764: DBGGBVR<n>\_EL1 bit descriptions**

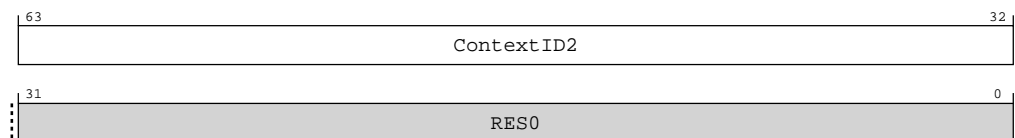
Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	VMID[7:0]	VMID value for comparison.	8 {x}
[31:0]	RES0	Reserved	RES0

When AArch64-DBGBCR<n>\_EL1.BT == '101'

**Figure A-303: AARCH64\_DBGGBVR<n>\_EL1 bit assignments****Table A-765: DBGGBVR<n>\_EL1 bit descriptions**

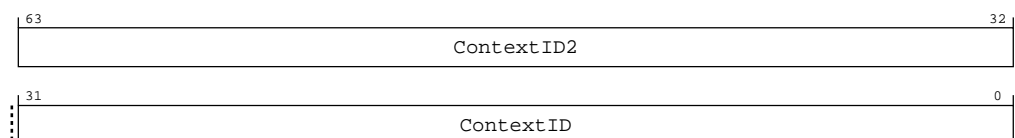
Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	VMID[7:0]	VMID value for comparison.	8 {x}
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32 {x}

When AArch64-DBGBCR<n>\_EL1.BT == '110'

**Figure A-304: AARCH64\_DBGGBVR<n>\_EL1 bit assignments****Table A-766: DBGGBVR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	ContextID2	Context ID value for comparison against AArch64-CONTEXTIDR_EL2.	32 {x}
[31:0]	RES0	Reserved	RES0

When AArch64-DBGBCR<n>\_EL1.BT == '111'

**Figure A-305: AARCH64\_DBGGBVR<n>\_EL1 bit assignments**

**Table A-767: DBGGBVR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	ContextID2	Context ID value for comparison against AArch64-CONTEXTIDR_EL2.	32{x}
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32{x}

**Access**

MRS &lt;Xt&gt;, DBGGBVR&lt;m&gt;\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b100

MSR DBGGBVR&lt;m&gt;\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b100

**Accessibility**

MRS &lt;Xt&gt;, DBGGBVR&lt;m&gt;\_EL1

```

integer m = UInt(CRm<3:0>);

if m >= 6 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGGBVR_EL1[m];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGGBVR_EL1[m];

```

MSR DBGGBVR&lt;m&gt;\_EL1, &lt;Xt&gt;

```

integer m = UInt(CRm<3:0>);

if m >= 6 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGGBVR_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);

```

```
else
    DBGBVR_EL1[m] = X[t, 64];
```

A.2.5.7 DBGBCR<n>\_EL1, Debug Breakpoint Control Registers, n = 0 - 5

Holds control information for a breakpoint. Forms breakpoint n together with value register AArch64-DBGBVR<n>\_EL1.

Configurations

If breakpoint n is not implemented, accesses to this register are UNDEFINED.

AArch64 register DBGBCR<n>\_EL1 bits [63:0] are architecturally mapped to External register [B.2.2.1.14 DBGBCR<n>\\_EL1, Debug Breakpoint Control Registers, n = 0 - 5](#) on page 1757 bits [63:0].

Attributes

Width

64

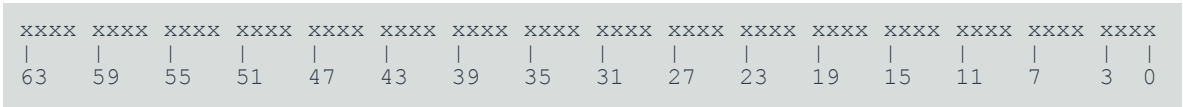
Functional group

Debug registers

Access type

See bit descriptions

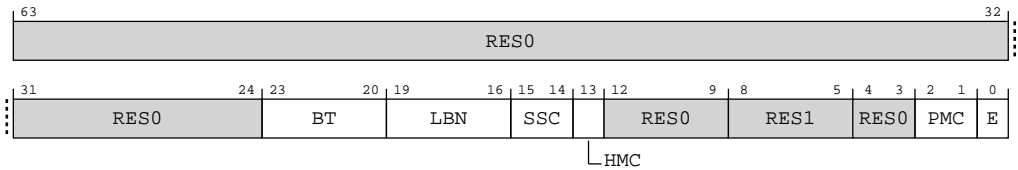
Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-306: AARCH64\_DBGBCR<n>\_EL1 bit assignments



**Table A-770: DBGBCR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:20]	BT	<p>Breakpoint Type.</p> <p>Specifies breakpoint type.</p> <p><b>0b0000</b> Unlinked instruction address match. AArch64-DBGBCR&lt;n&gt;_EL1 is the address of an instruction.</p> <p><b>0b0001</b> Linked instruction address match. As 0b0000, but linked to a breakpoint that has linking enabled.</p> <p><b>0b0010</b> Unlinked Context ID match. When FEAT_VHE is implemented, EL2 is using AArch64, the Effective value of AArch64-HCR_EL2.E2H is 1, and either the PE is executing at EL0 with AArch64-HCR_EL2.TGE set to 1 or the PE is executing at EL2, then AArch64-DBGBCR&lt;n&gt;_EL1.ContextID must match the AArch64-CONTEXTIDR_EL2 value. Otherwise, AArch64-DBGBCR&lt;n&gt;_EL1.ContextID must match the AArch64-CONTEXTIDR_EL1 value.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b0011</b> As 0b0010, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1000</b> Unlinked VMID match. AArch64-DBGBCR&lt;n&gt;_EL1.VMID is a VMID compared against AArch64-VTTBR_EL2.VMID.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1001</b> As 0b1000, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1010</b> Unlinked VMID and Context ID match. AArch64-DBGBCR&lt;n&gt;_EL1.ContextID is a Context ID compared against AArch64-CONTEXTIDR_EL1, and AArch64-DBGBCR&lt;n&gt;_EL1.VMID is a VMID compared against AArch64-VTTBR_EL2.VMID.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1011</b> As 0b1010, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p>	xxxx
[19:16]	LBN	<p>Linked Breakpoint Number.</p> <p>For Linked address matching breakpoints, specifies the index of the breakpoint linked to.</p> <p>For all other breakpoint types, this field is ignored and reads of the register return an <b>UNKNOWN</b> value.</p>	xxxx

Bits	Name	Description	Reset
[15:14]	SSC	<p>Security state control. Determines the Security states under which a Breakpoint debug event for breakpoint n is generated.</p> <p>The fields that indicate when the breakpoint can be generated are: HMC, PMC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>For more information on the effect of programming the fields to a reserved set of values, see <i>Reserved DBGBCR&lt;n&gt;_EL1.{SSC, HMC, PMC} values</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	xx
[13]	HMC	<p>Higher mode control. Determines the debug perspective for deciding when a Breakpoint debug event for breakpoint n is generated.</p> <p>The fields that indicate when the breakpoint can be generated are: HMC, PMC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>For more information, see DBGBCR&lt;n&gt;_EL1.SSC.</p>	x
[12:9]	RES0	Reserved	RES0
[8:5]	RES1	Reserved	RES1
[4:3]	RES0	Reserved	RES0
[2:1]	PMC	<p>Privilege mode control. Determines the Exception level or levels at which a Breakpoint debug event for breakpoint n is generated.</p> <p>The fields that indicate when the breakpoint can be generated are: HMC, PMC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>For more information, see DBGBCR&lt;n&gt;_EL1.SSC.</p>	xx
[0]	E	<p>Enable breakpoint n.</p> <p><b>0b0</b> Breakpoint n disabled.</p> <p><b>0b1</b> Breakpoint n enabled.</p>	x

## Access

MRS <Xt>, DBGBCR<m>\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b101

MSR DBGBCR<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b101

## Accessibility

MRS <Xt>, DBGBCR<m>\_EL1

```
integer m = UInt(CRm<3:0>);

if m >= 6 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGBCR_EL1[m];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGBCR_EL1[m];
```

MSR DBGBCR<m>\_EL1, <Xt>

```
integer m = UInt(CRm<3:0>);

if m >= 6 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGBCR_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGBCR_EL1[m] = X[t, 64];
```

### A.2.5.8 DBGWVR<n>\_EL1, Debug Watchpoint Value Registers, n = 0 - 3

Holds a data address value for use in watchpoint matching. Forms watchpoint n together with control register AArch64-DBGWCR<n>\_EL1.

## Configurations

If watchpoint n is not implemented then accesses to this register are UNDEFINED.

AArch64 register DBGWVR<n>\_EL1 bits [63:0] are architecturally mapped to External register [B.2.2.1.15 DBGWVR<n>\\_EL1, Debug Watchpoint Value Registers, n = 0 - 3](#) on page 1760 bits [63:0].

Attributes

Width

64

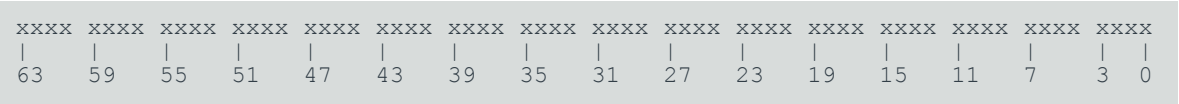
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-307: AARCH64\_DBGWVR<n>\_EL1 bit assignments

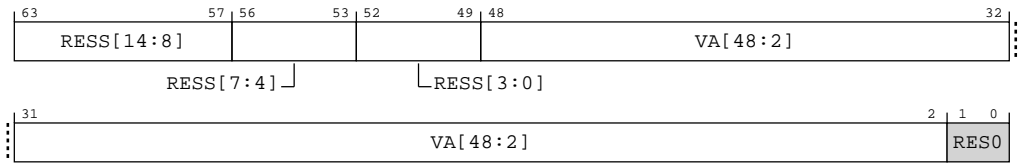


Table A-773: DBGWVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:57]	RESS[14:8]	Reserved, Sign extended. Software must set all bits in this field to the same value as the most significant bit of the VA field. If all bits in this field are not the same value as the most significant bit of the VA field, then the PE ignores this field when comparing an address, and if the breakpoint is not context-aware, the value read back in each bit of this field is a copy of the most significant bit of the VA field.	7 {x}
[56:53]	RESS[7:4]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[52:49]	RESS[3:0]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[48:2]	VA[48:2]	Bits[48:2] of the address value for comparison.  Arm deprecates setting AArch64-DBGWVR<n>_EL1[2] == 1.	47 {x}
[1:0]	RES0	Reserved	RES0



Access

MRS <Xt>, DBGWVR<m>\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b110

MSR DBGWVR<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b110

Accessibility

MRS <Xt>, DBGWVR<m>\_EL1

```
integer m = UInt(CRm<3:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGWVR_EL1[m];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGWVR_EL1[m];
```

MSR DBGWVR<m>\_EL1, <Xt>

```
integer m = UInt(CRm<3:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,tDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGWVR_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGWVR_EL1[m] = X[t, 64];
```

A.2.5.9 DBGWCR<n>\_EL1, Debug Watchpoint Control Registers, n = 0 - 3

Holds control information for a watchpoint. Forms watchpoint n together with value register AArch64-DBGWVR<n>\_EL1.

Configurations

If watchpoint n is not implemented then accesses to this register are UNDEFINED.

AArch64 register DBGWCR<n>\_EL1 bits [63:0] are architecturally mapped to External register [B.2.2.1.16 DBGWCR<n>\\_EL1, Debug Watchpoint Control Registers, n = 0 - 3](#) on page 1762 bits [63:0].

Attributes

Width

64

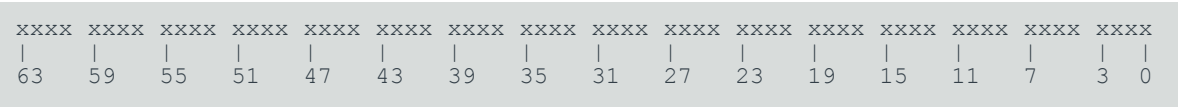
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-308: AARCH64\_DBGWCR<n>\_EL1 bit assignments

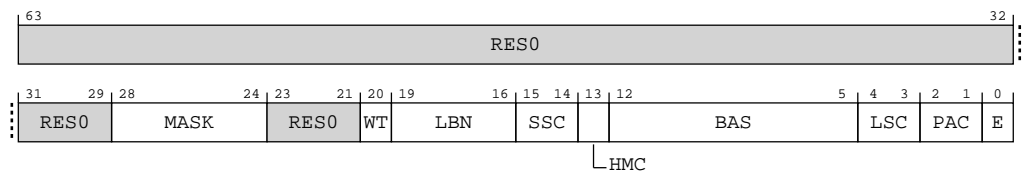


Table A-776: DBGWCR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:29]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[28:24]	MASK	<p>Address Mask. Only objects up to 2GB can be watched using a single mask.</p> <p><b>0b00000</b> No mask.</p> <p>All other values are reserved.</p> <p>Indicates the number of masked address bits, from 0b00011 masking 3 address bits (0x00000007 mask for address) to 0b11111 masking 31 address bits (0x7FFFFFFF mask for address).</p> <p>If programmed with a reserved value, the watchpoint behaves as if either:</p> <ul style="list-style-type: none"> <li>DBGWCR&lt;n&gt;_EL1.MASK has been programmed with a defined value, which might be 0 (no mask), other than for a direct read of DBGWCR&lt;n&gt;_EL1.</li> <li>The watchpoint is disabled.</li> </ul>	5 {x}
[23:21]	RES0	Reserved	RES0
[20]	WT	<p>Watchpoint type. Possible values are:</p> <p><b>0b0</b> Unlinked data address match.</p> <p><b>0b1</b> Linked data address match.</p>	x
[19:16]	LBN	<p>Linked Breakpoint Number.</p> <p>For Linked data address watchpoints, specifies the index of the breakpoint linked to.</p> <p>For all other watchpoint types, this field is ignored and reads of the register return an <b>UNKNOWN</b> value.</p>	xxxx
[15:14]	SSC	<p>Security state control. Determines the Security states under which a Watchpoint debug event for watchpoint n is generated.</p> <p>The fields that indicate when the watchpoint can be generated are: HMC, PAC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>For more information on the effect of programming the fields to a reserved value, see <i>Reserved DBGWCR&lt;n&gt;_EL1. {SSC, HMC, PAC} values</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	xx
[13]	HMC	<p>Higher mode control. Determines the debug perspective for deciding when a Watchpoint debug event for watchpoint n is generated.</p> <p>The fields that indicate when the watchpoint can be generated are: HMC, PAC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x

Bits	Name	Description	Reset
[12:5]	BAS	<p>Byte address select. Each bit of this field selects whether a byte from within the word or double-word addressed by AArch64-DBGWVR&lt;n&gt;_EL1 is being watched. <a href="#">Table A-777: BAS description</a> on page 1096</p> <p>In cases where AArch64-DBGWVR&lt;n&gt;_EL1 addresses a double-word: <a href="#">Table A-778: BAS description table 2</a> on page 1096</p> <p>If AArch64-DBGWVR&lt;n&gt;_EL1[2] == 1, only BAS[3:0] are used and BAS[7:4] are ignored. Arm deprecates setting AArch64-DBGWVR&lt;n&gt;_EL1[2] == 1.</p> <p>The valid values for BAS are nonzero binary numbers all of whose set bits are contiguous. All other values are reserved and must not be used by software. See <i>Reserved DBGWVR&lt;n&gt;_EL1.BAS values</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	8 {x}
[4:3]	LSC	<p>Load/store control. This field enables watchpoint matching on the type of access being made. Possible values of this field are:</p> <p><b>0b01</b> Match instructions that load from a watchpointed address.</p> <p><b>0b10</b> Match instructions that store to a watchpointed address.</p> <p><b>0b11</b> Match instructions that load from or store to a watchpointed address.</p> <p>All other values are reserved, but must behave as if the watchpoint is disabled. Software must not rely on this property as the behavior of reserved values might change in a future revision of the architecture.</p>	xx
[2:1]	PAC	<p>Privilege of access control. Determines the Exception level or levels at which a Watchpoint debug event for watchpoint n is generated.</p> <p>The fields that indicate when the watchpoint can be generated are: HMC, PAC, and SSC. These fields must be considered in combination, and the values that are permitted for these fields are constrained.</p> <p>For more information on the operation of these fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	xx
[0]	E	<p>Enable watchpoint n.</p> <p><b>0b0</b> Watchpoint n disabled.</p> <p><b>0b1</b> Watchpoint n enabled.</p>	x

**Table A-777: BAS description**

BAS	Description
xxxxxxx1	Match byte at AArch64-DBGWVR<n>_EL1
xxxxxx1x	Match byte at AArch64-DBGWVR<n>_EL1 + 1
xxxxx1xx	Match byte at AArch64-DBGWVR<n>_EL1 + 2
xxx1xxx	Match byte at AArch64-DBGWVR<n>_EL1 + 3

**Table A-778: BAS description table 2**

BAS	Description, if AArch64-DBGWVR<n>_EL1[2] == 0
xxx1xxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 4

BAS	Description, if AArch64-DBGWVR<n>_EL1[2] == 0
xx1xxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 5
x1xxxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 6
1xxxxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 7

## Access

MRS <Xt>, DBGWCR<m>\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b111

MSR DBGWCR<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0000	m[3:0]	0b111

## Accessibility

MRS <Xt>, DBGWCR<m>\_EL1

```
integer m = UInt(CRm<3:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGWCR_EL1[m];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        X[t, 64] = DBGWCR_EL1[m];
```

MSR DBGWCR<m>\_EL1, <Xt>

```
integer m = UInt(CRm<3:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
        DBGWCR_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if OSLSR_EL1.OSLK == '0' && HaltingAllowed() && EDSCR.TDA == '1' then
        Halt(DebugHalt_SoftwareAccess);
    else
```

```
DBGWCR_EL1[m] = X[t, 64];
```

A.2.5.10 MDRAR\_EL1, Monitor Debug ROM Address Register

Defines the base physical address of a 4KB-aligned memory-mapped debug component, usually a ROM table that locates and describes the memory-mapped debug components in the system. Armv8 deprecates any use of this register.

Configurations

This register is available in all configurations.

Attributes

Width

64

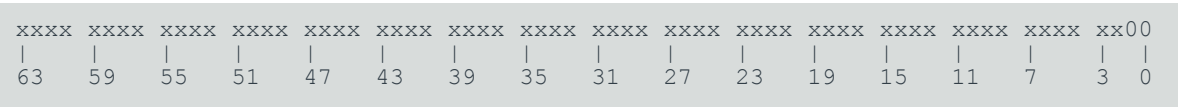
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-309: AARCH64\_MDRAR\_EL1 bit assignments

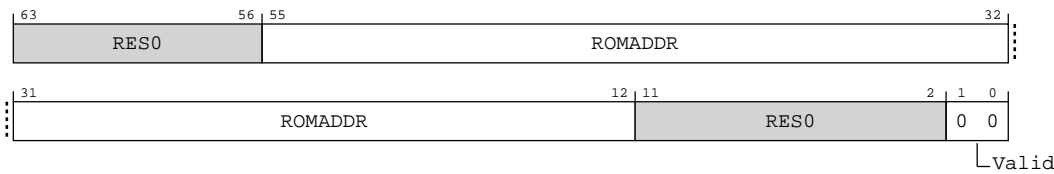


Table A-781: MDRAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0

Bits	Name	Description	Reset
55:12	ROMADDR	<b>ROMADDR encoding for None</b>  <b>43:0</b> Reserved, <b>UNKNOWN</b> .	44 {x}
[11:2]	RES0	Reserved	RES0
[1:0]	Valid	This field indicates whether the ROM Table address is valid.  <b>0b00</b> ROM Table address is not valid. Software must ignore ROMADDR.  Other values are reserved.  Arm recommends implementations set this field to zero.	0b00

### Access

MRS &lt;Xt&gt;, MDRAR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0000	0b000

### Accessibility

MRS &lt;Xt&gt;, MDRAR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDRA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = MDRAR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = MDRAR_EL1;

```

#### A.2.5.11 OSLAR\_EL1, OS Lock Access Register

Used to lock or unlock the OS Lock.

### Configurations

AArch64 register OSLAR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.10 OSLAR\\_EL1, OS Lock Access Register](#) on page 1744 bits [31:0].

### Attributes

#### Width

64

#### Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-310: AARCH64\_OSLAR\_EL1 bit assignments

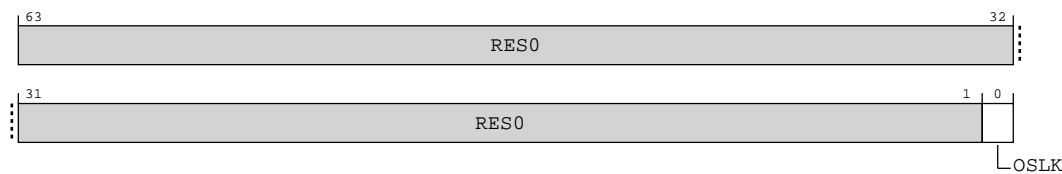


Table A-783: OSLAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	OSLK	On writes to OSLAR_EL1, bit[0] is copied to the OS Lock.  Use AArch64-OSLSR_EL1.OSLK to check the current status of the lock.	x

Access

MSR OSLAR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0000	0b100

Accessibility

MSR OSLAR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        OSLAR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    OSLAR_EL1 = X[t, 64];
```



A.2.5.12 OSLSR\_EL1, OS Lock Status Register

Provides the status of the OS Lock.

Configurations

This register is available in all configurations.

Attributes

Width

64

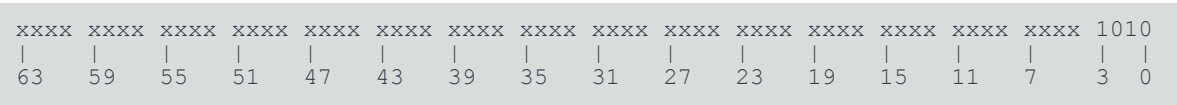
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-311: AARCH64\_OSLSR\_EL1 bit assignments

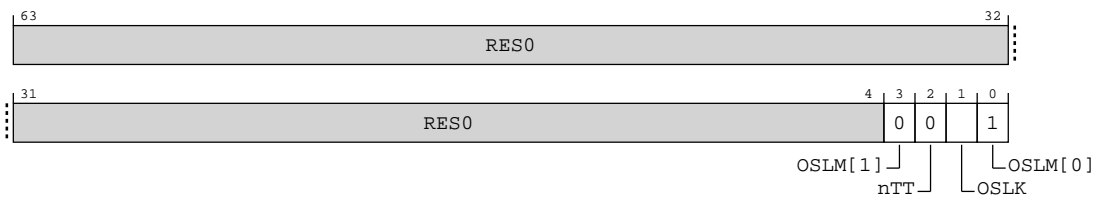


Table A-785: OSLSR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3, 0]	OSLM	OS Lock model implemented. Identifies the form of OS save and restore mechanism implemented.  0b10 OS Lock implemented.	0b10

Bits	Name	Description	Reset
[2]	nTT	Not 32-bit access. This bit is always <b>RAZ</b> . It indicates that a 32-bit access is needed to write the key to the OS Lock Access Register.  <b>0b0</b> 32-bit access.	0b0
[1]	OSLK	OS Lock Status.  <b>0b0</b> OS Lock unlocked.  <b>0b1</b> OS Lock locked.  The OS Lock is locked and unlocked by writing to the OS Lock Access Register.	0b1

Access

MRS <Xt>, OSLSR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0001	0b100

Accessibility

MRS <Xt>, OSLSR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = OSLSR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = OSLSR_EL1;
```

A.2.5.13 OSDLR\_EL1, OS Double Lock Register

Used to control the OS Double Lock.

Configurations

This register is available in all configurations.

Attributes

Width

64

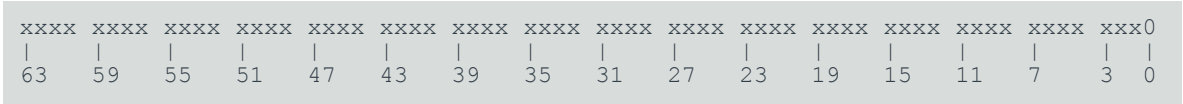
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-312: AARCH64\_OSDLR\_EL1 bit assignments

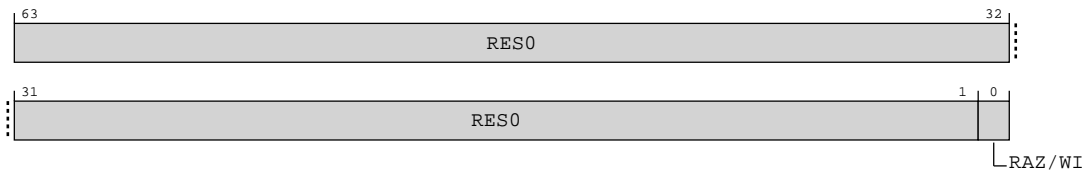


Table A-787: OSDLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Access

MRS <Xt>, OSDLR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0011	0b100

MSR OSDLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0011	0b100

Accessibility

MRS <Xt>, OSDLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = OSDLR_EL1;
elseif PSTATE.EL == EL2 then
```

X[t, 64] = OSDLR\_EL1;

MSR OSDLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        OSDLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    OSDLR_EL1 = X[t, 64];
```

A.2.5.14 DBGPRCR\_EL1, Debug Power Control Register

Controls behavior of the PE on powerdown request.

Configurations

Bit [0] of this register is mapped to ext-EDPRCR.CORENPDRQ, bit [0] of the external view of this register.

The other bits in these registers are not mapped to each other.

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-313: AARCH64\_DBGPRCR\_EL1 bit assignments

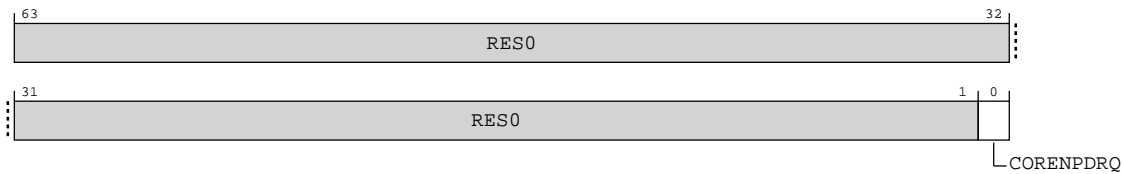


Table A-790: DBGPRCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	CORENPDRQ	<p>Core no powerdown request. Requests emulation of powerdown.</p> <p>This request is typically passed to an external power controller. This means that whether a request causes power up is dependent on the <b>IMPLEMENTATION DEFINED</b> nature of the system. The power controller must not allow the Core power domain to switch off while this bit is 1.</p> <p><b>0b0</b></p> <p>If the system responds to a powerdown request, it powers down Core power domain.</p> <p><b>0b1</b></p> <p>If the system responds to a powerdown request, it does not powerdown the Core power domain, but instead emulates a powerdown of that domain.</p> <p>This bit is not reset to the Cold reset value on exit from an <b>IMPLEMENTATION DEFINED</b> software-visible retention state.</p> <p><b>Note:</b></p> <p>Writes to this bit are not prohibited by the <b>IMPLEMENTATION DEFINED</b> authentication interface. This means that a debugger can request emulation of powerdown regardless of whether invasive debug is permitted.</p>	0b0

Access

MRS <Xt>, DBGPRCR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0100	0b100

MSR DBGPRCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0001	0b0100	0b100

Accessibility

MRS <Xt>, DBGPRCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGPRCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = DBGPRCR_EL1;
```


MSR DBGPRCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDOSA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGPRCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    DBGPRCR_EL1 = X[t, 64];
```

A.2.5.15 DBGCLAIMSET\_EL1, Debug CLAIM Tag Set Register

Used by software to set the CLAIM tag bits to 1.

The architecture does not define any functionality for the CLAIM tag bits.



Note

CLAIM tags are typically used for communication between the debugger and target software.

Used in conjunction with the AArch64-DBGCLAIMCLR\_EL1 register.

Configurations

An implementation must include eight CLAIM tag bits.

AArch64 register DBGCLAIMSET\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.22 DBGCLAIMSET\\_EL1, Debug CLAIM Tag Set Register](#) on page 1775 bits [31:0].

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

```
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx 0000 0000 0000 0000 0000 0000 xxxx xxxx
```



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-314: AARCH64\_DBGCLAIMSET\_EL1 bit assignments

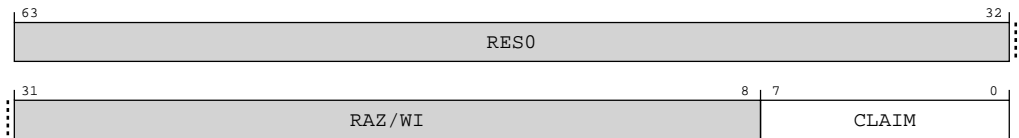


Table A-793: DBGCLAIMSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:8]	RAZ/WI	Reserved	RAZ/ WI
[7:0]	CLAIM	Set CLAIM tag bits.  This field is <b>RAO</b> .  Writing a 1 to one of these bits sets the corresponding CLAIM tag bit to 1. This is an indirect write to the CLAIM tag bits. A single write operation can set multiple CLAIM tag bits to 1.  Writing 0 to one of these bits has no effect.	8 {x}

Access

MRS <Xt>, DBGCLAIMSET\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0111	0b1000	0b110

MSR DBGCLAIMSET\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0111	0b1000	0b110

Accessibility

MRS <Xt>, DBGCLAIMSET\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```

elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGCLAIMSET_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = DBGCLAIMSET_EL1;

```

MSR DBGCLAIMSET\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGCLAIMSET_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    DBGCLAIMSET_EL1 = X[t, 64];

```

#### A.2.5.16 DBGCLAIMCLR\_EL1, Debug CLAIM Tag Clear Register

Used by software to read the values of the CLAIM tag bits, and to clear CLAIM tag bits to 0.

The architecture does not define any functionality for the CLAIM tag bits.



**Note**

CLAIM tags are typically used for communication between the debugger and target software.

Used in conjunction with the AArch64-DBGCLAIMSET\_EL1 register.

#### Configurations

An implementation must include eight CLAIM tag bits.

AArch64 register DBGCLAIMCLR\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.23 DBGCLAIMCLR\\_EL1, Debug CLAIM Tag Clear Register](#) on page 1777 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Debug registers

##### Access type

See bit descriptions

##### Reset value

```

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx 0000 0000 0000 0000 0000 0000 0000 0000

```





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-315: AARCH64\_DBGCLAIMCLR\_EL1 bit assignments

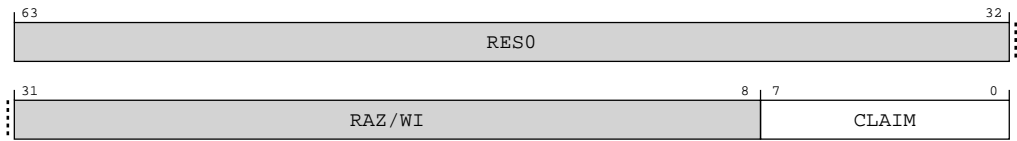


Table A-796: DBGCLAIMCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:8]	RAZ/WI	Reserved	RAZ/ WI
[7:0]	CLAIM	Read or clear CLAIM tag bits. Reading this field returns the current value of the CLAIM tag bits.  Writing a 1 to one of these bits clears the corresponding CLAIM tag bit to 0. This is an indirect write to the CLAIM tag bits. A single write operation can clear multiple CLAIM tag bits to 0.  Writing 0 to one of these bits has no effect.	0x00

Access

MRS <Xt>, DBGCLAIMCLR\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0111	0b1001	0b110

MSR DBGCLAIMCLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b000	0b0111	0b1001	0b110

Accessibility

MRS <Xt>, DBGCLAIMCLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
```

```
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGCLAIMCLR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = DBGCLAIMCLR_EL1;
```

MSR DBGCLAIMCLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGCLAIMCLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    DBGCLAIMCLR_EL1 = X[t, 64];
```

A.2.5.17 DBGAUTHSTATUS\_EL1, Debug Authentication Status Register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for debug.

Configurations

This register is in the Core power domain.

AArch64 register DBGAUTHSTATUS\_EL1 bits [31:0] are architecturally mapped to External register [B.2.2.1.28 DBGAUTHSTATUS\\_EL1, Debug Authentication Status Register](#) on page 1783 bits [31:0].

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-316: AARCH64\_DBGAUTHSTATUS\_EL1 bit assignments

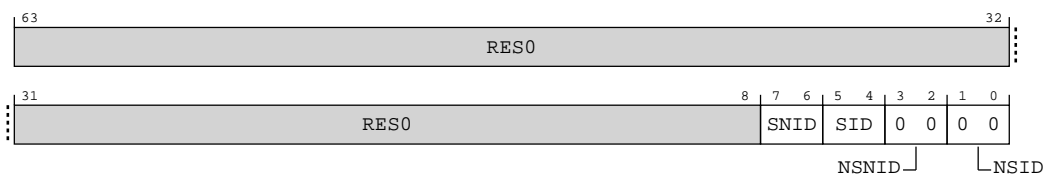


Table A-799: DBGAUTHSTATUS\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure non-invasive debug.  This field has the same value as DBGAUTHSTATUS_EL1.SID.	xx
[5:4]	SID	Secure invasive debug.  <b>0b10</b> Implemented and disabled. ExternalSecureInvasiveDebugEnabled() == FALSE.  <b>0b11</b> Implemented and enabled. ExternalSecureInvasiveDebugEnabled() == TRUE.  All other values are reserved.	xx
[3:2]	NSNID	Non-secure non-invasive debug.  <b>0b00</b> Non-secure state is not implemented.  All other values are reserved.	0b00
[1:0]	NSID	Non-secure invasive debug.  <b>0b00</b> Non-secure state is not implemented.  All other values are reserved.	0b00

Access

MRS <Xt>, DBGAUTHSTATUS\_EL1

op0	op1	CRn	CRm	op2
0b10	0b000	0b0111	0b1110	0b110

Accessibility

MRS <Xt>, DBGAUTHSTATUS\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
```

```
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGAUTHSTATUS_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = DBGAUTHSTATUS_EL1;
```

A.2.5.18 MDCCSR\_EL0, Monitor DCC Status Register

Read-only register containing control status flags for the DCC.

Configurations

AArch64 register MDCCSR\_EL0 bits [30:29] are architecturally mapped to External register [B.2.2.1.6 EDSCR, External Debug Status and Control Register](#) on page 1731 bits [30:29].

Attributes

Width

64

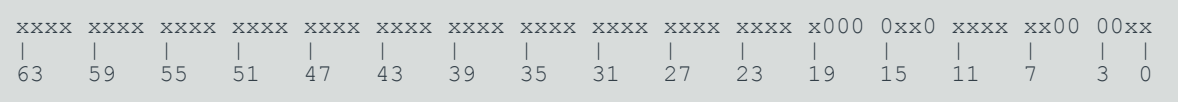
Functional group

Debug registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-317: AARCH64\_MDCCSR\_EL0 bit assignments

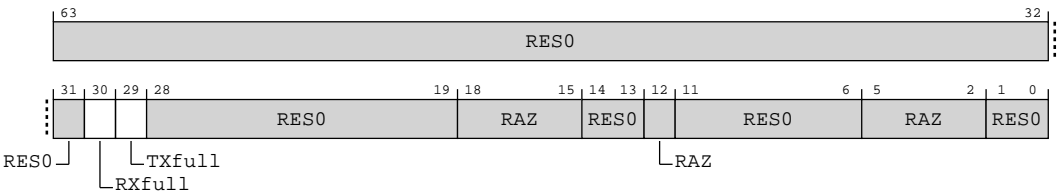


Table A-801: MDCCSR\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[30]	RXfull	DTRRX full. Read-only view of the equivalent bit in the ext-EDSCR.	x
[29]	TXfull	DTRTX full. Read-only view of the equivalent bit in the ext-EDSCR.	x
[28:19]	RES0	Reserved	RES0
[18:15]	RAZ	Reserved	RAZ
[14:13]	RES0	Reserved	RES0
[12]	RAZ	Reserved	RAZ
[11:6]	RES0	Reserved	RES0
[5:2]	RAZ	Reserved	RAZ
[1:0]	RES0	Reserved	RES0

## Access

MRS <Xt>, MDCCSR\_ELO

op0	op1	CRn	CRm	op2
0b10	0b011	0b0000	0b0001	0b000

## Accessibility

MRS <Xt>, MDCCSR\_ELO

```

if Halted() then
    X[t, 64] = MDCCSR_ELO;
elsif PSTATE.EL == EL0 then
    if MDSCR_EL1.TDCC == '1' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif HCR_EL2.TGE == '1' || MDCR_EL2.<TDE,TDA> != '00' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = MDCCSR_ELO;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.<TDE,TDA> != '00' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = MDCCSR_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = MDCCSR_ELO;

```

### A.2.5.19 DBGDTR\_ELO, Debug Data Transfer Register, half-duplex

Transfers 64 bits of data between the PE and an external debugger. Can transfer both ways using only a single register.

## Configurations

AArch64 register DBGDTR\_ELO bits [63:32] are architecturally mapped to External register [B.2.2.1.4 DBGDTRRX\\_ELO, Debug Data Transfer Register, Receive](#) on page 1728 bits [31:0].

AArch64 register DBGDTR\_ELO bits [63:32] are architecturally mapped to AArch64 System register [A.2.5.20 DBGDTRRX\\_ELO, Debug Data Transfer Register, Receive](#) on page 1116 bits [31:0].

AArch64 register DBGDTR\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.1.7 DBGDTRTX\\_ELO, Debug Data Transfer Register, Transmit](#) on page 1737 bits [31:0].

AArch64 register DBGDTR\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.21 DBGDTRTX\\_ELO, Debug Data Transfer Register, Transmit](#) on page 1118 bits [31:0].

AArch64 register DBGDTR\_ELO bits [63:32] are architecturally mapped to External register [B.2.2.1.7 DBGDTRTX\\_ELO, Debug Data Transfer Register, Transmit](#) on page 1737 bits [31:0].

AArch64 register DBGDTR\_ELO bits [63:32] are architecturally mapped to AArch64 System register [A.2.5.21 DBGDTRTX\\_ELO, Debug Data Transfer Register, Transmit](#) on page 1118 bits [31:0].

AArch64 register DBGDTR\_ELO bits [31:0] are architecturally mapped to External register [B.2.2.1.4 DBGDTRRX\\_ELO, Debug Data Transfer Register, Receive](#) on page 1728 bits [31:0].

AArch64 register DBGDTR\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.20 DBGDTRRX\\_ELO, Debug Data Transfer Register, Receive](#) on page 1116 bits [31:0].

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-318: AARCH64\_DBGDTR\_ELO bit assignments

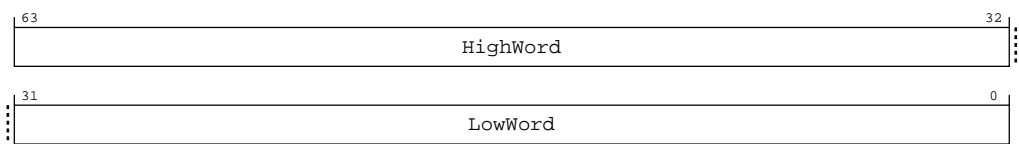


Table A-803: DBGDTR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	HighWord	<p>Writes to this register set DTRRX to the value in this field and do not change RXfull.</p> <p>Reads of this register:</p> <ul style="list-style-type: none"><li>If RXfull is set to 1, return the last value written to DTRTX.</li><li>If RXfull is set to 0, return an <b>UNKNOWN</b> value.</li></ul> <p>After the read, RXfull is cleared to 0.</p>	32 {x}
[31:0]	LowWord	<p>Writes to this register set DTRTX to the value in this field and set TXfull to 1.</p> <p>Reads of this register:</p> <ul style="list-style-type: none"><li>If RXfull is set to 1, return the last value written to DTRRX.</li><li>If RXfull is set to 0, return an <b>UNKNOWN</b> value.</li></ul> <p>After the read, RXfull is cleared to 0.</p>	32 {x}

Access

MRS <Xt>, DBGDTR\_ELO

op0	op1	CRn	CRm	op2
0b10	0b011	0b0000	0b0100	0b000

MSR DBGDTR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b011	0b0000	0b0100	0b000

Accessibility

MRS <Xt>, DBGDTR\_ELO

```
if Halted() then
    X[t, 64] = DBGDTR_ELO;
elseif PSTATE.EL == EL0 then
    if MDSCR_EL1.TDCC == '1' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elseif HCR_EL2.TGE == '1' || MDSCR_EL2.<TDE,TDA> != '00' then
```

```

        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGDTR_EL0;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.<TDE,TDA> != '00' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = DBGDTR_EL0;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = DBGDTR_EL0;

```

MSR DBGDTR\_EL0, &lt;Xt&gt;

```

if Halted() then
    DBGDTR_EL0 = X[t, 64];
elsif PSTATE.EL == EL0 then
    if MDSCR_EL1.TDCC == '1' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elsif HCR_EL2.TGE == '1' || MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGDTR_EL0 = X[t, 64];
elsif PSTATE.EL == EL1 then
    if MDCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGDTR_EL0 = X[t, 64];
elsif PSTATE.EL == EL2 then
    DBGDTR_EL0 = X[t, 64];

```

### A.2.5.20 DBGDTRRX\_EL0, Debug Data Transfer Register, Receive

Transfers data from an external debugger to the PE. For example, it is used by a debugger transferring commands and data to a debug target. See AArch64-DBGDTR\_EL0 for additional architectural mappings. It is a component of the Debug Communications Channel.

#### Configurations

AArch64 register DBGDTRRX\_EL0 bits [31:0] are architecturally mapped to External register [B.2.2.1.4 DBGDTRRX\\_EL0, Debug Data Transfer Register, Receive](#) on page 1728 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Debug registers

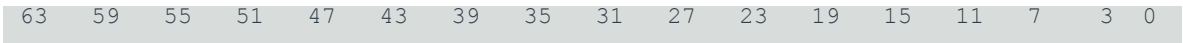
##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-319: AARCH64\_DBGDTRRX\_ELO bit assignments

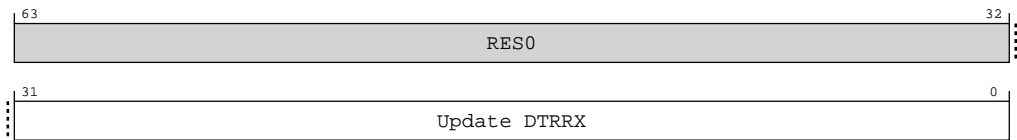


Table A-806: DBGDTRRX\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	None	Update DTRRX.  Reads of this register: <ul style="list-style-type: none"><li>If RXfull is set to 1, return the last value written to DTRRX.</li><li>If RXfull is set to 0, return an <b>UNKNOWN</b> value.</li></ul> After the read, RXfull is cleared to 0.  For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	32 {x}

Access

MRS <Xt>, DBGDTRRX\_ELO

op0	op1	CRn	CRm	op2
0b10	0b011	0b0000	0b0101	0b000

Accessibility

MRS <Xt>, DBGDTRRX\_ELO

```
if Halted() then
    X[t, 64] = DBGDTRRX_ELO;
elseif PSTATE.EL == EL0 then
    if MDSCR_EL1.TDCC == '1' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif HCR_EL2.TGE == '1' || MDSCR_EL2.<TDE,TDA> != '00' then
```

```
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = DBGDTRRX_EL0;
    elsif PSTATE.EL == EL1 then
        if MDCR_EL2.<TDE,TDA> != '00' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = DBGDTRRX_EL0;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = DBGDTRRX_EL0;
```

A.2.5.21 DBGDTRTX\_EL0, Debug Data Transfer Register, Transmit

Transfers data from the PE to an external debugger. For example, it is used by a debug target to transfer data to the debugger. See AArch64-DBGDTR\_EL0 for additional architectural mappings. It is a component of the Debug Communication Channel.

Configurations

AArch64 register DBGDTRTX\_EL0 bits [31:0] are architecturally mapped to External register [B.2.2.1.7 DBGDTRTX\\_EL0, Debug Data Transfer Register, Transmit](#) on page 1737 bits [31:0].

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

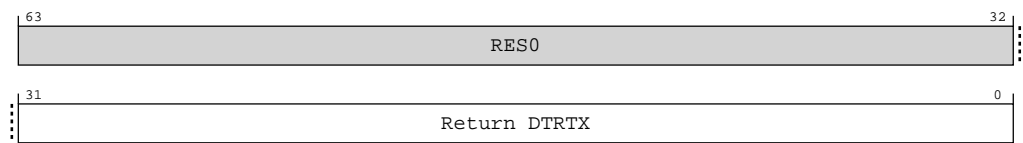
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-320: AARCH64\_DBGDTRTX\_EL0 bit assignments



**Table A-808: DBGDTRTX\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	None	Return DTRTX.  Writes to this register: <ul style="list-style-type: none"> <li>If TXfull is set to 1, set DTRRX and DTRTX to <b>UNKNOWN</b>.</li> <li>If TXfull is set to 0, update the value in DTRTX.</li> </ul> After the write, TXfull is set to 1.  For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	32 {x}

### Access

MSR DBGDTRTX\_ELO, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b011	0b0000	0b0101	0b000

### Accessibility

MSR DBGDTRTX\_ELO, &lt;Xt&gt;

```

if Halted() then
    DBGDTRTX_ELO = X[t, 64];
elseif PSTATE.EL == EL0 then
    if MDSCR_EL1.TDCC == '1' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif HCR_EL2.TGE == '1' || MDSCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGDTRTX_ELO = X[t, 64];
elseif PSTATE.EL == EL1 then
    if MDSCR_EL2.<TDE,TDA> != '00' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        DBGDTRTX_ELO = X[t, 64];
elseif PSTATE.EL == EL2 then
    DBGDTRTX_ELO = X[t, 64];

```

#### A.2.5.22 TRFCR\_EL1, Trace Filter Control Register (EL1)

Provides EL1 controls for Trace.

### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-321: AARCH64\_TRFCR\_EL1 bit assignments

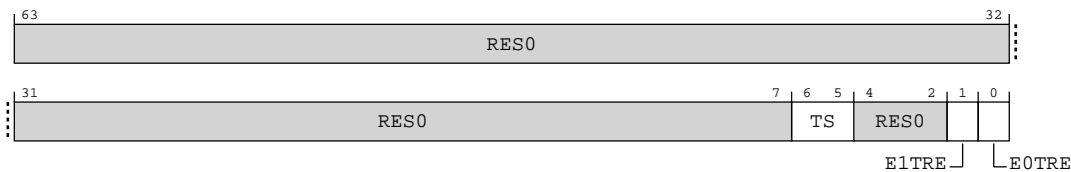


Table A-810: TRFCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:7]	RES0	Reserved	RES0
[6:5]	TS	Timestamp Control. Controls which timebase is used for trace timestamps.  <b>0b01</b> Virtual timestamp. The traced timestamp is the physical counter value minus the value of AArch64-CNTVOFF_EL2.  <b>0b11</b> Physical timestamp. The traced timestamp is the physical counter value.  All other values are reserved.  This field is ignored by the PE when any of the following are true: <ul style="list-style-type: none"><li>EL2 is implemented and AArch64-TRFCR_EL2.TS != 0b00.</li><li>SelfHostedTraceEnabled() == FALSE.</li></ul>	xx
[4:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1]	E1TRE	EL1 Trace Enable.  <b>0b0</b> Trace is prohibited at EL1.  <b>0b1</b> Trace is allowed at EL1.  This field is ignored if <code>SelfHostedTraceEnabled() == FALSE</code> .	0b0
[0]	E0TRE	ELO Trace Enable.  <b>0b0</b> Trace is prohibited at ELO.  <b>0b1</b> Trace is allowed at ELO.  This field is ignored if any of the following are true: <ul style="list-style-type: none"><li><code>SelfHostedTraceEnabled() == FALSE</code>.</li><li>EL2 is implemented and enabled in the current Security state and <code>AArch64-HCR_EL2.TGE == 1</code>.</li></ul>	0b0

Access

MRS <Xt>, TRFCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0010	0b001

MSR TRFCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0001	0b0010	0b001

Accessibility

MRS <Xt>, TRFCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TTRF == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRFCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = TRFCR_EL1;
```

MSR TRFCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if MDCR_EL2.TTRF == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

```
TRFCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    TRFCR_EL1 = X[t, 64];
```

A.2.5.23 MDCR\_EL2, Monitor Debug Configuration Register (EL2)

Provides EL2 configuration options for self-hosted debug and the Performance Monitors Extension.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx0x	xxxx	xxxx	xxx0	0110
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-322: AARCH64\_MDCR\_EL2 bit assignments

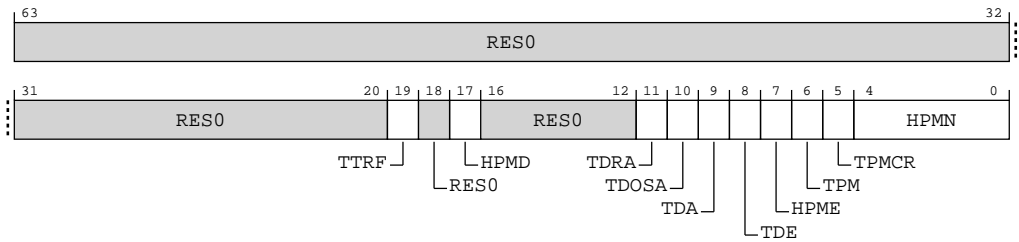


Table A-813: MDCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[19]	TTRF	<p>Traps use of the Trace Filter Control registers at EL1 to EL2, as follows:</p> <ul style="list-style-type: none"> <li>Access to AArch64-TRFCR_EL1 is trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>Accesses to the specified registers at EL1 are not affected by this control.</p> <p><b>0b1</b></p> <p>Accesses to the specified registers at EL1 generate a trap exception to EL2 when EL2 is enabled in the current Security state.</p>	x
[18]	RES0	Reserved	RES0
[17]	HPMD	<p>Guest Performance Monitors Disable. Controls PMU operation at EL2.</p> <p><b>0b0</b></p> <p>Counters are not affected by this mechanism.</p> <p><b>0b1</b></p> <p>Affected counters are prohibited from counting at EL2.</p> <p>If AArch64-PMCR_ELO.DP is 1, then AArch64-PMCCNTR_ELO is disabled at EL2. Otherwise, AArch64-PMCCNTR_ELO is not affected by this mechanism.</p> <p>The counters affected by this field are:</p> <ul style="list-style-type: none"> <li>Event counters AArch64-PMEVCNTR&lt;n&gt;_ELO for values of n less than MDCR_EL2.HPMN.</li> <li>If AArch64-PMCR_ELO.DP is 1, the cycle counter AArch64-PMCCNTR_ELO.</li> </ul> <p>Other event counters are not affected by this field.</p> <p>When AArch64-PMCR_ELO.DP is 0, AArch64-PMCCNTR_ELO is not affected by this field.</p>	0b0
[16:12]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[11]	TDRA	<p>Trap Debug ROM Address register access. Traps System register accesses to the Debug ROM registers to EL2 when EL2 is enabled in the current Security state as follows:</p> <ul style="list-style-type: none"> <li>If EL1 is using AArch64 state, accesses to AArch64-MDRAR_EL1 are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL0 and EL1 System register accesses to the Debug ROM registers are trapped to EL2 when EL2 is enabled in the current Security state, unless it is trapped by the following:</p> <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.TDCC.</li> </ul> <p>This field is treated as being 1 for all purposes other than a direct read when one or more of the following are true:</p> <ul style="list-style-type: none"> <li>AArch64-MDCR_EL2.TDE == 1.</li> <li>AArch64-HCR_EL2.TGE == 1.</li> </ul> <p><b>Note:</b> EL2 does not provide traps on debug register accesses through the optional memory-mapped external debug interfaces.</p> <p>System register accesses to the debug registers might have side-effects. When a System register access is trapped to EL2, no side-effects occur before the exception is taken to EL2.</p>	x
[10]	TDOSA	<p>Trap debug OS-related register access. Traps EL1 System register accesses to the powerdown debug registers to EL2, from both Execution states as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to the following registers are trapped to EL2, reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-OSLAR_EL1, AArch64-OSLSR_EL1, AArch64-OSDLR_EL1, and AArch64-DBGPRCR_EL1.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>EL1 System register accesses to the powerdown debug registers are trapped to EL2.</p> <p><b>Note:</b> These registers are not accessible at EL0.</p> <p>This field is treated as being 1 for all purposes other than a direct read when one or more of the following are true:</p> <ul style="list-style-type: none"> <li>AArch64-MDCR_EL2.TDE == 1.</li> <li>AArch64-HCR_EL2.TGE == 1.</li> </ul> <p><b>Note:</b> EL2 does not provide traps on debug register accesses through the optional memory-mapped external debug interfaces.</p> <p>System register accesses to the debug registers might have side-effects. When a System register access is trapped to EL2, no side-effects occur before the exception is taken to EL2.</p>	x



Bits	Name	Description	Reset
[9]	TDA	<p>Trap accesses of debug System registers. Enables a trap to EL2 on accesses of debug System registers.</p> <p><b>0b0</b></p> <p>Accesses of the specified debug System registers are not trapped by this mechanism.</p> <p><b>0b1</b></p> <p>Accesses of the specified debug System registers at EL1 and EL0 are trapped to EL2, unless the instruction generates a higher priority exception.</p> <p>In AArch64 state, the instructions affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS and MSR accesses to AArch64-DBGAUTHSTATUS_EL1, AArch64-DBGBCR&lt;n&gt;_EL1, AArch64-DBGBVR&lt;n&gt;_EL1, AArch64-DBGCLAIMCLR_EL1, AArch64-DBGCLAIMSET_EL1, AArch64-DBGWCR&lt;n&gt;_EL1, AArch64-DBGWVR&lt;n&gt;_EL1, AArch64-MDCCINT_EL1, AArch64-MDCCSR_EL0, AArch64-MDSCR_EL1, AArch64-OSDTRRX_EL1, AArch64-OSDTRTX_EL1, and AArch64-OSECCR_EL1.</li> <li>In Non-debug state, MRS accesses to AArch64-DBGDTRRX_EL0 and AArch64-DBGDTR_EL0 and MSR accesses to AArch64-DBGDTRTX_EL0 and AArch64-DBGDTR_EL0.</li> </ul> <p>Unless the instruction generates a higher priority exception, trapped instructions generate an exception to EL2.</p> <p>Trapped AArch64 instructions are reported using EC syndrome value 0x18.</p> <p>The following instructions are not trapped in Debug state:</p> <ul style="list-style-type: none"> <li>AArch64 MRS accesses to AArch64-DBGDTRRX_EL0 and AArch64-DBGDTR_EL0 and MSR accesses to AArch64-DBGDTRTX_EL0 and AArch64-DBGDTR_EL0.</li> <li>AArch32 MRC accesses to AArch32-DBGDTRRXint and MCR accesses to AArch32-DBGDTRTXint.</li> </ul> <p>This field is ignored by the PE and treated as one when any of the following are true:</p> <ul style="list-style-type: none"> <li>MDCR_EL2.TDE == 1.</li> <li>AArch64-HCR_EL2.TGE == 1.</li> </ul>	x
[8]	TDE	<p>Trap Debug Exceptions. Controls routing of Debug exceptions, and defines the debug target Exception level, EL<sub>D</sub>.</p> <p><b>0b0</b></p> <p>The debug target Exception level is EL1.</p> <p><b>0b1</b></p> <p>If EL2 is enabled for the current Effective value of AArch64-SCR_EL3.NS, the debug target Exception level is EL2, otherwise the debug target Exception level is EL1.</p> <p>The MDCR_EL2.{TDRA, TDOSA, TDA} fields are treated as being 1 for all purposes other than returning the result of a direct read of the register.</p> <p>For more information, see <i>Routing debug exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>This field is treated as being 1 for all purposes other than a direct read when AArch64-HCR_EL2.TGE == 1.</p>	x

Bits	Name	Description	Reset
[7]	HPME	<p>Hyp Enable.</p> <p><b>0b0</b></p> <p>Affected counters are disabled and do not count.</p> <p><b>0b1</b></p> <p>Affected counters are enabled by AArch64-PMCNTENSET_ELO.</p> <p>The counters affected by this field are event counters AArch64-PMEVCNTR&lt;n&gt;_ELO for values of n greater than or equal to MDCR_EL2.HPMN and less than AArch64-PMCR_ELO.N.</p> <p>Other event counters and AArch64-PMCCNTR_ELO are not affected by this field.</p> <p>If MDCR_EL2.HPMN is equal to AArch64-PMCR_ELO.N, then this field has no effect.</p>	x
[6]	TPM	<p>Trap accesses of PMU registers. Enables a trap to EL2 on accesses of PMU registers.</p> <p><b>0b0</b></p> <p>Accesses of the specified PMU registers are not trapped by this mechanism.</p> <p><b>0b1</b></p> <p>Accesses of the specified PMU registers at EL1 and ELO are trapped to EL2, unless the instruction generates a higher priority exception.</p> <p>In AArch64 state, the instructions affected by this control are:</p> <ul style="list-style-type: none"> <li>MRS and MSR accesses to AArch64-PMCCFILTR_ELO, AArch64-PMCCNTR_ELO, AArch64-PMCNTENCLR_ELO, AArch64-PMCNTENSET_ELO, AArch64-PMCR_ELO, AArch64-PMEVCNTR&lt;n&gt;_ELO, AArch64-PMEVTYPER&lt;n&gt;_ELO, AArch64-PMINTENCLR_EL1, AArch64-PMINTENSET_EL1, AArch64-PMOVSLR_ELO, AArch64-PMOVSSET_ELO, AArch64-PMSELR_ELO, AArch64-PMSWINC_ELO, AArch64-PMUSERENR_ELO, AArch64-PMXEVCNTR_ELO, and AArch64-PMXEVTYPER_ELO.</li> <li>MRS accesses to AArch64-PMCEIDO_ELO and AArch64-PMCEID1_ELO.</li> <li>If FEAT_PMUV3p4 is implemented, MRS accesses to AArch64-PMMIR_EL1.</li> </ul> <p>Unless the instruction generates a higher priority exception, trapped instructions generate an exception to EL2.</p> <p>Trapped AArch64 instructions are reported using EC syndrome value 0x18.</p>	x
[5]	TPMCR	<p>Trap AArch64-PMCR_ELO or AArch32-PMCR accesses. Traps ELO and EL1 accesses to EL2, when EL2 is enabled in the current Security state, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to AArch64-PMCR_ELO are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <p><b>0b0</b></p> <p>This control does not cause any instructions to be trapped.</p> <p><b>0b1</b></p> <p>ELO and EL1 accesses to the specified registers are trapped to EL2 when EL2 is enabled in the current Security state, unless they are trapped by the following:</p> <ul style="list-style-type: none"> <li>AArch64-PMUSERENR_ELO.EN.</li> </ul> <p><b>Note:</b></p> <p>EL2 does not provide traps on Performance Monitor register accesses through the optional memory-mapped external debug interface.</p>	x

Bits	Name	Description	Reset
[4:0]	HPMN	<p>Defines the number of event counters AArch64-PMEVCNTR&lt;n&gt;_ELO that are accessible from EL1 and from ELO if permitted.</p> <p>MDCR_EL2.HPMN divides the event counters into a first range and a second range.</p> <p>If MDCR_EL2.HPMN is not 0 and is less than AArch64-PMCR_ELO.N, then event counters [0..(MDCR_EL2.HPMN-1)] are in the first range, and the remaining event counters [MDCR_EL2.HPMN..(AArch64-PMCR_ELO.N-1)] are in the second range.</p> <p>If MDCR_EL2.HPMN is equal to AArch64-PMCR_ELO.N, then all event counters are in the first range and none are in the second range.</p> <p>For an event counter AArch64-PMEVCNTR&lt;n&gt;_ELO in the first range:</p> <ul style="list-style-type: none"> <li>The counter is accessible from EL1 and EL2.</li> <li>The counter is accessible from ELO if permitted by AArch64-PMUSERENR_ELO.</li> <li>AArch64-PMCR_ELO.E and AArch64-PMCNTENSET_ELO[n] enable the operation of the event counter.</li> </ul> <p>For an event counter AArch64-PMEVCNTR&lt;n&gt;_ELO in the second range:</p> <ul style="list-style-type: none"> <li>The counter is only accessible from EL2.</li> <li>MDCR_EL2.HPME and AArch64-PMCNTENSET_ELO[n] enable the operation of the event counter.</li> </ul> <p>Values greater than AArch64-PMCR_ELO.N and 0 are reserved.</p> <p>If this field is set to a reserved value, then the following CONSTRAINED UNPREDICTABLE behaviors apply:</p> <ul style="list-style-type: none"> <li>The value returned by a direct read of MDCR_EL2.HPMN is <b>UNKNOWN</b>.</li> <li>Either: <ul style="list-style-type: none"> <li>An <b>UNKNOWN</b> number of counters are reserved for EL2 use. That is, the PE behaves as if MDCR_EL2.HPMN is set to an <b>UNKNOWN</b> nonzero value less than or equal to AArch64-PMCR_ELO.N.</li> <li>All counters are reserved for EL2 use, meaning no counters are accessible from EL1 and ELO.</li> </ul> </li> </ul>	0b00110

## Access

MRS <Xt>, MDCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b001

MSR MDCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b001

## Accessibility

MRS <Xt>, MDCR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
```

```
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = MDCR_EL2;
```

MSR MDCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    MDCR_EL2 = X[t, 64];
```

A.2.5.24 TRFCR\_EL2, Trace Filter Control Register (EL2)

Provides EL2 controls for Trace.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Debug registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x00x	0x00
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-323: AARCH64\_TRFCR\_EL2 bit assignments

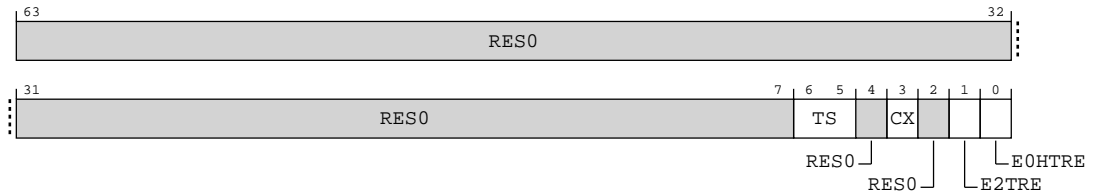


Table A-816: TRFCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:7]	RES0	Reserved	RES0
[6:5]	TS	<p>Timestamp Control. Controls which timebase is used for trace timestamps.</p> <p><b>0b00</b> Timestamp controlled by AArch64-TRFCR_EL1.TS.</p> <p><b>0b01</b> Virtual timestamp. The traced timestamp is the physical counter value minus the value of AArch64-CNTVOFF_EL2.</p> <p><b>0b11</b> Physical timestamp. The traced timestamp is the physical counter value.</p> <p>This field is ignored by the PE when <code>SelfHostedTraceEnabled() == FALSE</code>.</p>	0b00
[4]	RES0	Reserved	RES0
[3]	CX	<p>AArch64-CONTEXTIDR_EL2 and VMID trace enable.</p> <p><b>0b0</b> AArch64-CONTEXTIDR_EL2 and VMID trace prohibited.</p> <p><b>0b1</b> AArch64-CONTEXTIDR_EL2 and VMID trace allowed.</p> <p>This field is ignored if <code>SelfHostedTraceEnabled() == FALSE</code>.</p>	0b0
[2]	RES0	Reserved	RES0
[1]	E2TRE	<p>EL2 Trace Enable.</p> <p><b>0b0</b> Trace is prohibited at EL2.</p> <p><b>0b1</b> Trace is allowed at EL2.</p> <p>This field is ignored if <code>SelfHostedTraceEnabled() == FALSE</code>.</p>	0b0

Bits	Name	Description	Reset
[0]	EOHTRE	EL0 Trace Enable.  <b>0b0</b> Trace is prohibited at EL0 when AArch64-HCR_EL2.TGE == 1.  <b>0b1</b> Trace is allowed at EL0 when AArch64-HCR_EL2.TGE == 1.  This field is ignored if any of the following are true: <ul style="list-style-type: none"><li>SelfHostedTraceEnabled() == FALSE.</li><li>AArch64-HCR_EL2.TGE == 0.</li></ul>	0b0

**Access**  
MRS <Xt>, TRFCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0010	0b001

MSR TRFCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0010	0b001

**Accessibility**  
MRS <Xt>, TRFCR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = TRFCR_EL2;
```

MSR TRFCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    TRFCR_EL2 = X[t, 64];
```

A.2.6 AArch64 GIC register description

This section includes the register descriptions for all *Generic Interrupt Controller* (GIC) registers in the Cortex®-R82AE processor.

A.2.6.1 ICC\_PMR\_EL1, Interrupt Controller Interrupt Priority Mask Register

Provides an interrupt priority filter. Only interrupts with a higher priority than the value in this register are signaled to the PE.

Writes to this register must be high performance and must ensure that no interrupt of lower priority than the written value occurs after the write, without requiring an ISB or an exception boundary.

Configurations

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that writes to this register are self-synchronising. This ensures that no interrupts below the written PMR value will be taken after a write to this register is architecturally executed. For more information, see 'Observability of the effects of accesses to the GIC registers' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

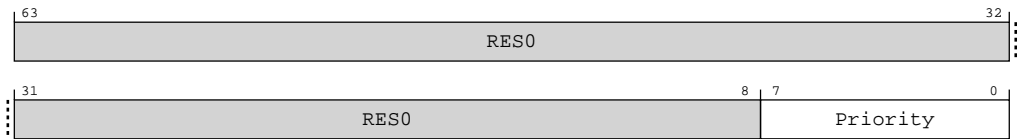


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-324: AARCH64\_ICC\_PMR\_EL1 bit assignments



**Table A-819: ICC\_PMR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	Priority	<p>The priority mask level for the CPU interface. If the priority of an interrupt is higher than the value indicated by this field, the interface signals the interrupt to the PE.</p> <p>The implemented priority field values are as follows: <a href="#">Table A-820: Implemented priority bits description</a> on page 1132</p> <p>Unimplemented priority bits are <b>RAZ/WI</b>.</p>	0x00

**Table A-820: Implemented priority bits description**

Implemented priority bits	Possible priority field values	Number of priority levels
[7:3]	0b00-F8 (0-248), in steps of 8	32

### Access

MRS &lt;Xt&gt;, ICC\_PMR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0110	0b000

MSR ICC\_PMR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0110	0b000

### Accessibility

MRS &lt;Xt&gt;, ICC\_PMR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_PMR_EL1;
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_PMR_EL1;
    else
        X[t, 64] = ICC_PMR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_PMR_EL1;

```

MSR ICC\_PMR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_PMR_EL1 = X[t, 64];

```



```
elseif HCR_EL2.IMO == '1' then
    ICV_PMR_EL1 = X[t, 64];
else
    ICC_PMR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_PMR_EL1 = X[t, 64];
```

A.2.6.2 ICV\_PMR\_EL1, Interrupt Controller Virtual Interrupt Priority Mask Register

Provides a virtual interrupt priority filter. Only virtual interrupts with a higher priority than the value in this register are signaled to the PE.

Configurations

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that writes to this register are self-synchronising. This ensures that no interrupts below the written PMR value will be taken after a write to this register is architecturally executed. For more information, see 'Observability of the effects of accesses to the GIC registers' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

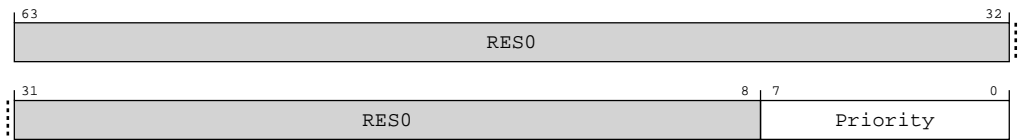


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-325: AARCH64\_ICV\_PMR\_EL1 bit assignments



**Table A-823: ICV\_PMR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	Priority	The priority mask level for the virtual CPU interface. If the priority of a virtual interrupt is higher than the value indicated by this field, the interface signals the virtual interrupt to the PE.  The possible priority field values are as follows: <a href="#">Table A-824: Implemented priority bits description</a> on page 1134  Unimplemented priority bits are <b>RAZ/WI</b> .	0x00

**Table A-824: Implemented priority bits description**

Implemented priority bits	Possible priority field values	Number of priority levels
[7:3]	0b00-F8 (0-248), in steps of 8	32

### Access

MRS &lt;Xt&gt;, ICC\_PMR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0110	0b000

MSR ICC\_PMR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0110	0b000

### Accessibility

MRS &lt;Xt&gt;, ICC\_PMR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_PMR_EL1;
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_PMR_EL1;
    else
        X[t, 64] = ICC_PMR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_PMR_EL1;

```

MSR ICC\_PMR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_PMR_EL1 = X[t, 64];
    elseif HCR_EL2.IMO == '1' then
        ICV_PMR_EL1 = X[t, 64];

```

```
else
    ICC_PMR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_PMR_EL1 = X[t, 64];
```

A.2.6.3 ICC\_IAR0\_EL1, Interrupt Controller Interrupt Acknowledge Register 0

The PE reads this register to obtain the INTID of the signaled Group 0 interrupt. This read acts as an acknowledge for the interrupt.

Configurations

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that reads of this register are self-synchronising when interrupts are masked by the PE (that is when PSTATE.{I,F} == {0,0}). This ensures that the effect of activating an interrupt on the signaling of interrupt exceptions is observed when a read of this register is architecturally executed so that no spurious interrupt exception occurs if interrupts are unmasked by an instruction immediately following the read. For more information, see 'Observability of the effects of accesses to the GIC registers'.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

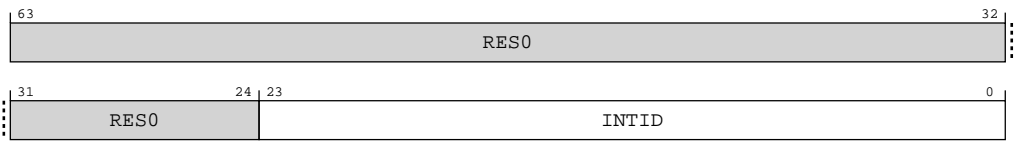
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-326: AARCH64\_ICC\_IAR0\_EL1 bit assignments



**Table A-827: ICC\_IAR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:0]	<b>INTID</b>	<p>The INTID of the signaled interrupt.</p> <p>This is the INTID of the highest priority pending interrupt, if that interrupt is of sufficient priority for it to be signaled to the PE, and if it can be acknowledged at the current Security state and Exception level.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p>	24 {x}

### Access

MRS &lt;Xt&gt;, ICC\_IAR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b000

### Accessibility

MRS &lt;Xt&gt;, ICC\_IAR0\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_IAR0_EL1;
    else
        X[t, 64] = ICC_IAR0_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_IAR0_EL1;

```

## A.2.6.4 ICV\_IAR0\_EL1, Interrupt Controller Virtual Interrupt Acknowledge Register 0

The PE reads this register to obtain the INTID of the signaled virtual Group 0 interrupt. This read acts as an acknowledge for the interrupt.

### Configurations

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that reads of this register are self-synchronising when interrupts are masked by the PE (that is when PSTATE.{I,F} == {0,0}). This ensures that the effect of activating an interrupt on the signaling of interrupt exceptions is observed when a read of this register is architecturally executed so that no spurious interrupt exception occurs if interrupts are unmasked by an instruction immediately following the read. For more information,

see 'Observability of the effects of accesses to the GIC registers' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

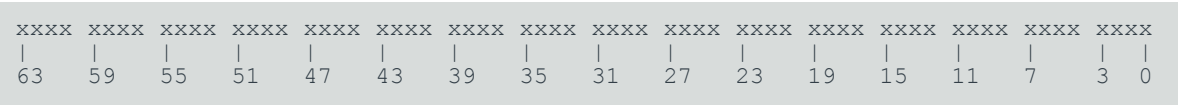
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-327: AARCH64\_ICV\_IAR0\_EL1 bit assignments

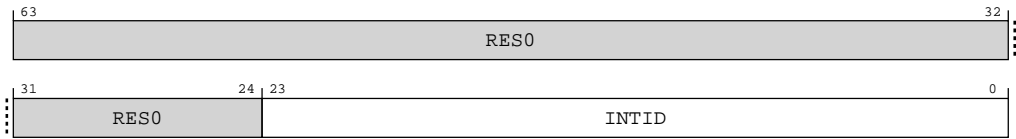


Table A-829: ICV\_IAR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	<p>The INTID of the signaled virtual interrupt.</p> <p>This is the INTID of the highest priority pending virtual interrupt, if that interrupt is of sufficient priority for it to be signaled to the PE, and if it can be acknowledged.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p>	24 {x}

Access

MRS <Xt>, ICC\_IAR0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b000

Accessibility

MRS <Xt>, ICC\_IAR0\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_IAR0_EL1;
    else
        X[t, 64] = ICC_IAR0_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_IAR0_EL1;
```

A.2.6.5 ICC\_EOIR0\_EL1, Interrupt Controller End Of Interrupt Register 0

A PE writes to this register to inform the CPU interface that it has completed the processing of the specified Group 0 interrupt.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-328: AARCH64\_ICC\_EOIR0\_EL1 bit assignments

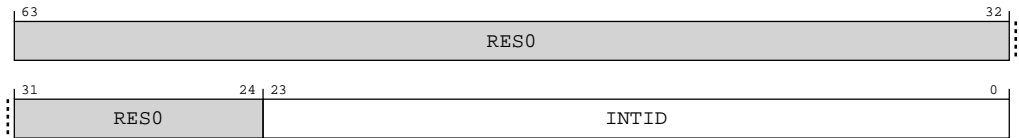


Table A-831: ICC\_EOIR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	<p>The INTID from the corresponding AArch64-ICC_IAR0_EL1 access.</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p> <p>If AArch64-ICC_CTLR_EL1.EOIMode is 0, a write to this register drops the priority for the interrupt, and also deactivates the interrupt.</p> <p>If AArch64-ICC_CTLR_EL1.EOIMode is 1, a write to this register only drops the priority for the interrupt and software must write to AArch64-ICC_DIR_EL1 to deactivate the interrupt.</p>	24 {x}

Access

A write to this register must correspond to the most recent valid read by this PE from an Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICC\_IAR0\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

A write of a Special INTID is ignored. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

MSR ICC\_EOIR0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b001

Accessibility

A write to this register must correspond to the most recent valid read by this PE from an Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICC\_IAR0\_EL1, otherwise the system behavior is UNPREDICTABLE. A valid read is a read that returns a valid INTID that is not a special INTID.

A write of a Special INTID is ignored. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

MSR ICC\_EOIRO\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        ICV_EOIRO_EL1 = X[t, 64];
    else
        ICC_EOIRO_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ICC_EOIRO_EL1 = X[t, 64];
```

A.2.6.6 ICV\_EOIRO\_EL1, Interrupt Controller Virtual End Of Interrupt Register 0

A PE writes to this register to inform the CPU interface that it has completed the processing of the specified virtual Group 0 interrupt.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

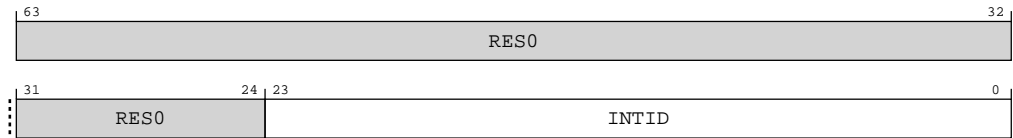


Where the reset reads xxxx, see individual bits.



## Bit descriptions

**Figure A-329: AARCH64\_ICV\_EOIR0\_EL1 bit assignments**



**Table A-833: ICV\_EOIR0\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	<p>The INTID from the corresponding AArch64-ICV_IAR0_EL1 access.</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p> <p>If the AArch64-ICV_CTLR_EL1.EOImode bit is 0, a write to this register drops the priority for the virtual interrupt, and also deactivates the virtual interrupt.</p> <p>If the AArch64-ICV_CTLR_EL1.EOImode bit is 1, a write to this register only drops the priority for the virtual interrupt. Software must write to AArch64-ICV_DIR_EL1 to deactivate the virtual interrupt.</p>	24 {x}

## Access

A write to this register must correspond to the most recent valid read by this vPE from a Virtual Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICV\_IAR0\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

MSR ICC\_EOIR0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b001

## Accessibility

A write to this register must correspond to the most recent valid read by this vPE from a Virtual Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICV\_IAR0\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

MSR ICC\_EOIR0\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        ICV_EOIR0_EL1 = X[t, 64];
    else
        ICC_EOIR0_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then

```

```
ICC_EOIR0_EL1 = X[t, 64];
```

### A.2.6.7 ICC\_AP0R<n>\_EL1, Interrupt Controller Active Priorities Group 0 Registers, n = 0

Provides information about Group 0 active priorities.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

GIC system registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

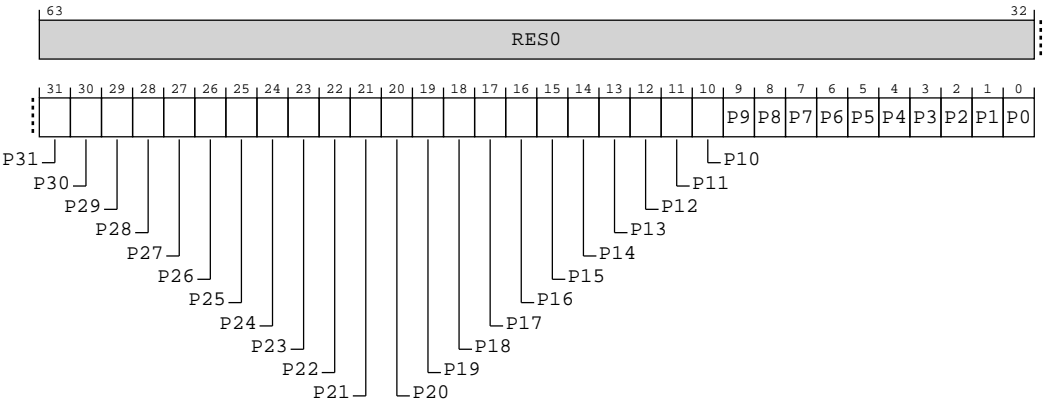


Note

Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-330: AARCH64\_ICC\_AP0R<n>\_EL1 bit assignments



**Table A-835: ICC\_AP0R<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	P<x>, bit[x], where x = 31 to 0	Provides the access to the active priorities for Group 0 interrupts. Possible values of each bit are:  <b>0b0</b>  There is no Group 0 interrupt active with priority level x * 8, or all active Group 0 interrupts with this priority level have undergone priority-drop.  <b>0b1</b>  There is a Group 0 interrupt active with priority level x * 8 which has not undergone priority drop.	0x00000000

The contents of these registers are **IMPLEMENTATION DEFINED** with the one architectural requirement that the value 0x00000000 is consistent with no interrupts being active.

### Access

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 0 active priorities) might result in **UNPREDICTABLE** behavior of the interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

Writing to the active priority registers in any order other than the following order will result in **UNPREDICTABLE** behavior:

- AArch64-ICC\_AP0R<n>\_EL1.
- AArch64-ICC\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP0R<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	'1':m[1:0]

MSR ICC\_AP0R<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	'1':m[1:0]

### Accessibility

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 0 active priorities) might result in **UNPREDICTABLE** behavior of the interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

Writing to the active priority registers in any order other than the following order will result in UNPREDICTABLE behavior:

- AArch64-ICC\_AP0R<n>\_EL1.
- AArch64-ICC\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP0R<m>\_EL1

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_AP0R_EL1[m];
    else
        X[t, 64] = ICC_AP0R_EL1[m];
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_AP0R_EL1[m];
```

MSR ICC\_AP0R<m>\_EL1, <Xt>

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_AP0R_EL1[m] = X[t, 64];
    else
        ICC_AP0R_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_AP0R_EL1[m] = X[t, 64];
```

### A.2.6.8 ICV\_AP0R<n>\_EL1, Interrupt Controller Virtual Active Priorities Group 0 Registers, n = 0

Provides information about virtual Group 0 active priorities.

#### Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-331: AARCH64\_ICV\_AP0R<n>\_EL1 bit assignments

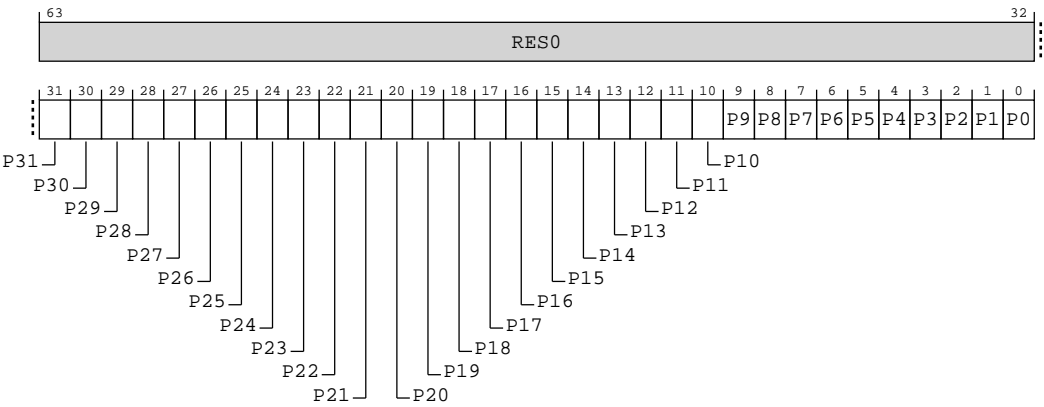


Table A-838: ICV\_AP0R<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:0]	P<x>, bit[x], where x = 31 to 0	Provides the access to the active priorities for virtual Group 0 interrupts. Possible values of each bit are:  <b>0b0</b> There is no virtual Group 0 interrupt active with priority level $x * 8$ , or all active Group 0 interrupts with this priority level have undergone priority-drop.  <b>0b1</b> There is a virtual Group 0 interrupt active with priority level $x * 8$ which has not undergone priority drop.	32 {x}

The contents of these registers are **IMPLEMENTATION DEFINED** with the one architectural requirement that the value 0x00000000 is consistent with no interrupts being active.

### Access

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 0 active priorities) might result in **UNPREDICTABLE** behavior of the virtual interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

ICV\_AP0R1\_EL1 is implemented only in implementations that support 6 or more bits of priority. ICV\_AP0R2\_EL1 and ICV\_AP0R3\_EL1 are implemented only in implementations that support 7 bits of priority. Unimplemented registers are **UNDEFINED**.

Writing to the active priority registers in any order other than the following order might result in **UNPREDICTABLE** behavior of the interrupt prioritization system:

- ICV\_AP0R<n>\_EL1.
- AArch64-ICV\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP0R<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	'1':m[1:0]

MSR ICC\_AP0R<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	'1':m[1:0]

### Accessibility

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 0 active priorities) might result in **UNPREDICTABLE** behavior of the virtual interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

ICV\_AP0R1\_EL1 is implemented only in implementations that support 6 or more bits of priority. ICV\_AP0R2\_EL1 and ICV\_AP0R3\_EL1 are implemented only in implementations that support 7 bits of priority. Unimplemented registers are UNDEFINED.

Writing to the active priority registers in any order other than the following order might result in UNPREDICTABLE behavior of the interrupt prioritization system:

- ICV\_AP0R<n>\_EL1.
- AArch64-ICV\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP0R<m>\_EL1

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_AP0R_EL1[m];
    else
        X[t, 64] = ICC_AP0R_EL1[m];
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_AP0R_EL1[m];
```

MSR ICC\_AP0R<m>\_EL1, <Xt>

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_AP0R_EL1[m] = X[t, 64];
    else
        ICC_AP0R_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_AP0R_EL1[m] = X[t, 64];
```

#### A.2.6.9 ICC\_HPPIRO\_EL1, Interrupt Controller Highest Priority Pending Interrupt Register 0

Indicates the highest priority pending Group 0 interrupt on the CPU interface.

#### Configurations

This register is available in all configurations.

Attributes

Width

64

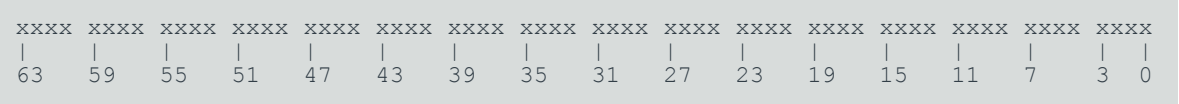
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-332: AARCH64\_ICC\_HPPIRO\_EL1 bit assignments

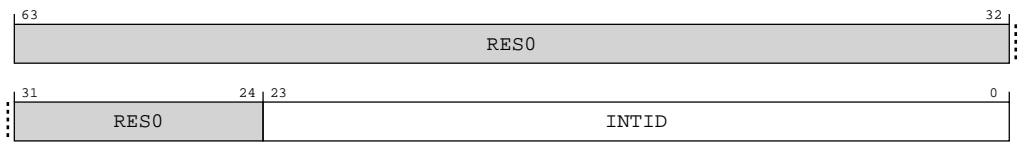


Table A-841: ICC\_HPPIRO\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	The INTID of the highest priority pending interrupt, if that interrupt is observable at the current Security state and Exception level.  If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. These special INTIDs can be one of: 1020, 1021, or 1023. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).  Bits [23:16] of this register are RES0.	24 {x}

Access

MRS <Xt>, ICC\_HPPIRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b010



Accessibility

MRS <Xt>, ICC\_HPPIRO\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_HPPIRO_EL1;
    else
        X[t, 64] = ICC_HPPIRO_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ICC_HPPIRO_EL1;
```

A.2.6.10 ICV\_HPPIRO\_EL1, Interrupt Controller Virtual Highest Priority Pending Interrupt Register 0

Indicates the highest priority pending virtual Group 0 interrupt on the virtual CPU interface.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-333: AARCH64\_ICV\_HPPIRO\_EL1 bit assignments

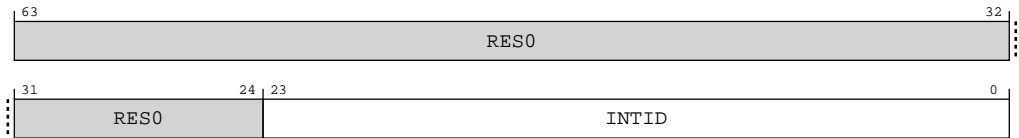


Table A-843: ICV\_HPPIRO\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	<p>The INTID of the highest priority pending virtual interrupt.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. This special INTID can take the value 1023 only. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p>	24 {x}

Access

MRS <Xt>, ICC\_HPPIRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b010

Accessibility

MRS <Xt>, ICC\_HPPIRO\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_HPPIRO_EL1;
    else
        X[t, 64] = ICC_HPPIRO_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_HPPIRO_EL1;
```

A.2.6.11 ICV\_BPRO\_EL1, Interrupt Controller Virtual Binary Point Register 0

Defines the point at which the priority value fields split into two parts, the group priority field and the subpriority field. The group priority field determines virtual Group 0 interrupt preemption.

Configurations

This register is available in all configurations.

Attributes

Width

64

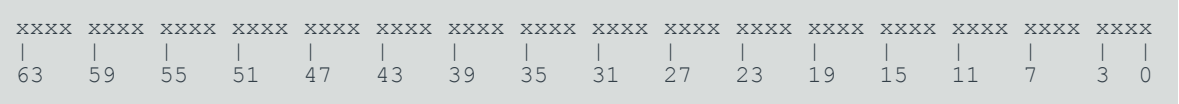
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-334: AARCH64\_ICV\_BPR0\_EL1 bit assignments

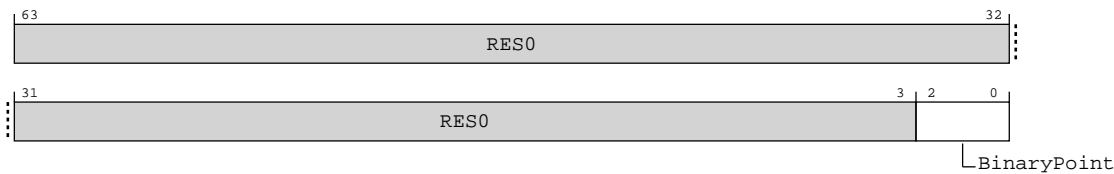


Table A-845: ICV\_BPR0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0
[2:0]	BinaryPoint	The value of this field controls how the 8-bit interrupt priority field is split into a group priority field, that determines interrupt preemption, and a subpriority field. This is done as follows: <a href="#">Table A-846: Binary point value description</a> on page 1151	xxx

Table A-846: Binary point value description

Binary point value	Group priority field	Subpriority field	Field with binary point
2	[7:3]	[2:0]	ggggg.sss
3	[7:4]	[3:0]	gggg.ssss
4	[7:5]	[4:0]	ggg.sssss
5	[7:6]	[5:0]	gg.ssssss
6	[7]	[6:0]	g.sssssss
7	No preemption	[7:0]	.ssssssss

Access

The minimum binary point value is derived from the number of implemented preemption bits, as shown in the following table:

Table A-847: Number of implemented preemption bits description

Number of implemented preemption bits	Minimum value of BPRO
7	0
6	1
5	2

The number of implemented preemption bits is indicated by AArch64-ICH\_VTR\_EL2.PREbits.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value. On a reset, the binary point field is **UNKNOWN**.

MRS <Xt>, ICC\_BPRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b011

MSR ICC\_BPRO\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1000	0b011

Accessibility

The minimum binary point value is derived from the number of implemented preemption bits, as shown in the following table:

+-----+-----+   Number of implemented preemption bits   Minimum value of BPRO   +=====
+=====+   7   0   +-----
+-----+   6   1   +-----+-----+   5   2
+-----+-----+-----+

The number of implemented preemption bits is indicated by AArch64-ICH\_VTR\_EL2.PREbits.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value. On a reset, the binary point field is UNKNOWN.

MRS <Xt>, ICC\_BPRO\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_BPRO_EL1;
    else
```

```
        X[t, 64] = ICC_BPRO_EL1;
    elif PSTATE.EL == EL2 then
        X[t, 64] = ICC_BPRO_EL1;
```

MSR ICC\_BPRO\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elif HCR_EL2.FMO == '1' then
        ICV_BPRO_EL1 = X[t, 64];
    else
        ICC_BPRO_EL1 = X[t, 64];
elif PSTATE.EL == EL2 then
    ICC_BPRO_EL1 = X[t, 64];
```

A.2.6.12 ICC\_AP1R<n>\_EL1, Interrupt Controller Active Priorities Group 1 Registers, n = 0

Provides information about Group 1 active priorities.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

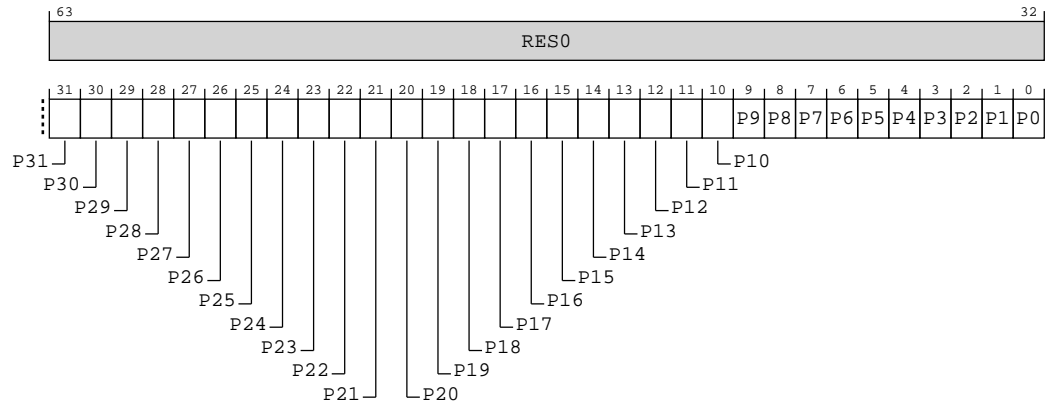


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-335: AARCH64\_ICC\_AP1R<n>\_EL1 bit assignments**



**Table A-850: ICC\_AP1R<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	P<x>, bit[x], where x = 31 to 0	Provides the access to the active priorities for Group 1 interrupts. Possible values of each bit are:  <b>0b0</b>  There is no Group 1 interrupt active with priority level x * 8, or all active Group 0 interrupts with this priority level have undergone priority-drop.  <b>0b1</b>  There is a Group 1 interrupt active with priority level x * 8 which has not undergone priority drop.	0x00000000

The contents of these registers are **IMPLEMENTATION DEFINED** with the one architectural requirement that the value 0x00000000 is consistent with no interrupts being active.

### Access

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 1 active priorities) might result in **UNPREDICTABLE** behavior of the interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

Writing to the active priority registers in any order other than the following order will result in **UNPREDICTABLE** behavior:

- AArch64-ICC\_AP0R<n>\_EL1.
- AArch64-ICC\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP1R<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1001	'0':m[1:0]

MSR ICC\_AP1R<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1001	'0':m[1:0]

## Accessibility

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 1 active priorities) might result in UNPREDICTABLE behavior of the interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

Writing to the active priority registers in any order other than the following order will result in UNPREDICTABLE behavior:

- AArch64-ICC\_AP0R<n>\_EL1.
- AArch64-ICC\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP1R<m>\_EL1

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_AP1R_EL1[m];
    else
        X[t, 64] = ICC_AP1R_EL1[m];
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_AP1R_EL1[m];
```

MSR ICC\_AP1R<m>\_EL1, <Xt>

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        ICV_AP1R_EL1[m] = X[t, 64];
```

```
else
    ICC_AP1R_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_AP1R_EL1[m] = X[t, 64];
```

### A.2.6.13 ICV\_AP1R<n>\_EL1, Interrupt Controller Virtual Active Priorities Group 1 Registers, n = 0

Provides information about virtual Group 1 active priorities.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

GIC system registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

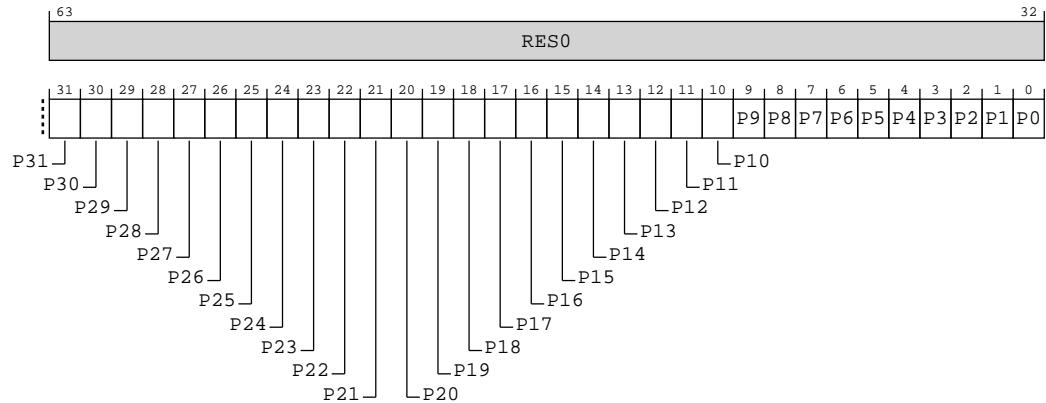


Where the reset reads xxxx, see individual bits.



## Bit descriptions

**Figure A-336: AARCH64\_ICV\_AP1R<n>\_EL1 bit assignments**



**Table A-853: ICV\_AP1R<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	P<x>, bit[x], where x = 31 to 0	<p>Provides the access to the active priorities for virtual Group 1 interrupts. Possible values of each bit are:</p> <p><b>0b0</b></p> <p>There is no virtual Group 1 interrupt active with priority level <math>x * 8</math>, or all active Group 1 interrupts with this priority level have undergone priority-drop.</p> <p><b>0b1</b></p> <p>There is a virtual Group 1 interrupt active with priority level <math>x * 8</math> which has not undergone priority drop.</p>	32 {x}

The contents of these registers are **IMPLEMENTATION DEFINED** with the one architectural requirement that the value 0x00000000 is consistent with no interrupts being active.

### Access

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 1 active priorities) might result in **UNPREDICTABLE** behavior of the virtual interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

ICV\_AP1R1\_EL1 is implemented only in implementations that support 6 or more bits of priority. ICV\_AP1R2\_EL1 and ICV\_AP1R3\_EL1 are implemented only in implementations that support 7 bits of priority. Unimplemented registers are **UNDEFINED**.

Writing to the active priority registers in any order other than the following order might result in **UNPREDICTABLE** behavior of the interrupt prioritization system:

- AArch64-ICV\_APOR<n>\_EL1.

- ICV\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP1R<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1001	'0':m[1:0]

MSR ICC\_AP1R<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1001	'0':m[1:0]

Accessibility

Writing to these registers with any value other than the last read value of the register (or 0x00000000 when there are no Group 1 active priorities) might result in UNPREDICTABLE behavior of the virtual interrupt prioritization system, causing:

- Interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution.

ICV\_AP1R1\_EL1 is implemented only in implementations that support 6 or more bits of priority. ICV\_AP1R2\_EL1 and ICV\_AP1R3\_EL1 are implemented only in implementations that support 7 bits of priority. Unimplemented registers are UNDEFINED.

Writing to the active priority registers in any order other than the following order might result in UNPREDICTABLE behavior of the interrupt prioritization system:

- AArch64-ICV\_APOR<n>\_EL1.
- ICV\_AP1R<n>\_EL1.

MRS <Xt>, ICC\_AP1R<m>\_EL1

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_AP1R_EL1[m];
    else
        X[t, 64] = ICC_AP1R_EL1[m];
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_AP1R_EL1[m];
```

MSR ICC\_AP1R<m>\_EL1, <Xt>

```
integer m = UInt(op2<1:0>);
```

```
if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        ICV_AP1R_EL1[m] = X[t, 64];
    else
        ICC_AP1R_EL1[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_AP1R_EL1[m] = X[t, 64];
```

A.2.6.14 ICC\_DIR\_EL1, Interrupt Controller Deactivate Interrupt Register

When interrupt priority drop is separated from interrupt deactivation, a write to this register deactivates the specified interrupt.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-337: AARCH64\_ICC\_DIR\_EL1 bit assignments

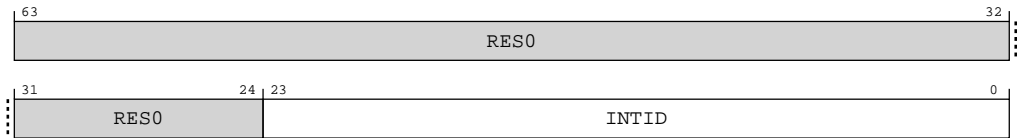


Table A-856: ICC\_DIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	The INTID of the interrupt to be deactivated. Bits [23:16] of this register are <b>RES0</b> .	24 {x}

Access

There are two cases when writing to AArch64-ICC\_DIR\_EL1 that were **UNPREDICTABLE** for a corresponding GICv2 write to ext-GICC\_DIR:

- When EOImode == 0. GICv3 implementations must ignore such writes. In systems supporting system error generation, an implementation might generate an SEI.
- When EOImode == 1 but no EOI has been issued. The interrupt will be de-activated by the Distributor, however the active priority in the CPU interface for the interrupt will remain set (because no EOI was issued).

MSR ICC\_DIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b001

Accessibility

There are two cases when writing to AArch64-ICC\_DIR\_EL1 that were UNPREDICTABLE for a corresponding GICv2 write to ext-GICC\_DIR:

- When EOImode == 0. GICv3 implementations must ignore such writes. In systems supporting system error generation, an implementation might generate an SEI.
- When EOImode == 1 but no EOI has been issued. The interrupt will be de-activated by the Distributor, however the active priority in the CPU interface for the interrupt will remain set (because no EOI was issued).

MSR ICC\_DIR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TDIR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        ICDIR_EL1 = X[t, 64];
```

```
elseif HCR_EL2.IMO == '1' then
    ICV_DIR_EL1 = X[t, 64];
else
    ICC_DIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_DIR_EL1 = X[t, 64];
```

A.2.6.15 ICV\_DIR\_EL1, Interrupt Controller Deactivate Virtual Interrupt Register

When interrupt priority drop is separated from interrupt deactivation, a write to this register deactivates the specified virtual interrupt.

Configurations

This register is available in all configurations.

Attributes

Width

64

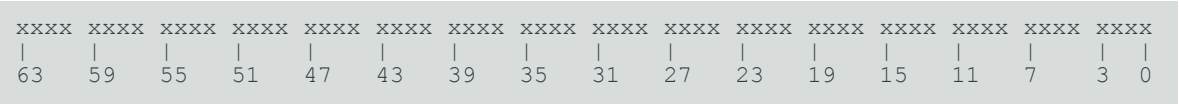
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-338: AARCH64\_ICV\_DIR\_EL1 bit assignments

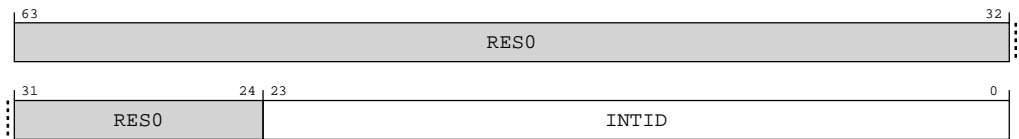


Table A-858: ICV\_DIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[23:0]	INTID	The INTID of the interrupt to be deactivated. Bits [23:16] of this register are <b>RESO</b> .	24{x}

### Access

When EOImode == 0, writes are ignored. In systems supporting system error generation, an implementation might generate an SEI.

MSR ICC\_DIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b001

### Accessibility

When EOImode == 0, writes are ignored. In systems supporting system error generation, an implementation might generate an SEI.

MSR ICC\_DIR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TDIR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_DIR_EL1 = X[t, 64];
    elseif HCR_EL2.IMO == '1' then
        ICV_DIR_EL1 = X[t, 64];
    else
        ICC_DIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_DIR_EL1 = X[t, 64];

```

## A.2.6.16 ICC\_RPR\_EL1, Interrupt Controller Running Priority Register

Indicates the Running priority of the CPU interface.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

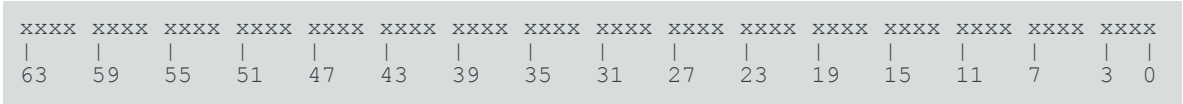
#### Functional group

GIC system registers

#### Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-339: AARCH64\_ICC\_RPR\_EL1 bit assignments

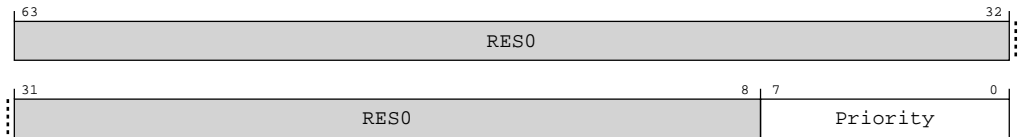


Table A-860: ICC\_RPR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	Priority	<p>The current running priority on the CPU interface. This is the group priority of the current active interrupt.</p> <p>The group priority of a Secure NMI, or NMI when GICD_CTLR.DS is 1, is 0x00. The group priority of a Non-secure NMI is 0x80, saturated to 0x00 for Non-secure reads.</p> <p>If there are no active interrupts on the CPU interface, or all active interrupts have undergone a priority drop, the value returned is the Idle priority.</p> <p>The priority returned is the group priority as if the BPR for the current Exception level and Security state was set to the minimum value of BPR for the number of implemented priority bits.</p> <p><b>Note:</b> If 8 bits of priority are implemented the group priority is bits[7:1] of the priority.</p>	8 {x}

Access

Software cannot determine the number of implemented priority bits from a read of this register.

MRS <Xt>, ICC\_RPR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b011

Accessibility

Software cannot determine the number of implemented priority bits from a read of this register.

MRS <Xt>, ICC\_RPR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_RPR_EL1;
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_RPR_EL1;
    else
        X[t, 64] = ICC_RPR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ICC_RPR_EL1;
```

A.2.6.17 ICV\_RPR\_EL1, Interrupt Controller Virtual Running Priority Register

Indicates the Running priority of the virtual CPU interface.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-340: AARCH64\_ICV\_RPR\_EL1 bit assignments

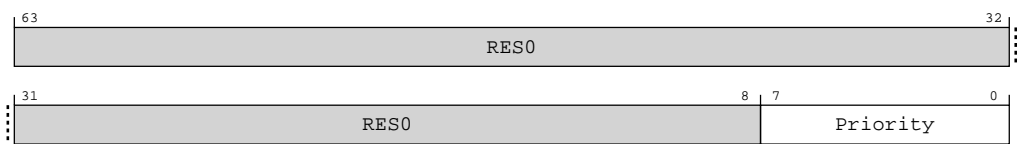


Table A-862: ICV\_RPR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	Priority	<p>The current running priority on the virtual CPU interface. This is the group priority of the current active virtual interrupt.</p> <p>If there are no active interrupts on the virtual CPU interface, or all active interrupts have undergone a priority drop, the value returned is the Idle priority.</p> <p>The priority returned is the group priority as if the BPR for the current Exception level and Security state was set to the minimum value of BPR for the number of implemented priority bits.</p> <p><b>Note:</b> If 8 bits of priority are implemented the group priority is bits[7:1] of the priority.</p>	8 {x}

Access

If there are no active interrupts on the virtual CPU interface, or all active interrupts have undergone a priority drop, the value returned is the Idle priority.

Software cannot determine the number of implemented priority bits from a read of this register.

MRS <Xt>, ICC\_RPR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b011

Accessibility

If there are no active interrupts on the virtual CPU interface, or all active interrupts have undergone a priority drop, the value returned is the Idle priority.

Software cannot determine the number of implemented priority bits from a read of this register.

MRS <Xt>, ICC\_RPR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
```

```

        X[t, 64] = ICV_RPR_EL1;
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_RPR_EL1;
    else
        X[t, 64] = ICC_RPR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_RPR_EL1;

```

A.2.6.18 ICC\_SGI1R\_EL1, Interrupt Controller Software Generated Interrupt Group 1 Register

Generates Group 1 SGIs for the current Security state.

Configurations

Under certain conditions a write to ICC\_SGI1R\_EL1 can generate Group 0 interrupts, see 'Forwarding an SGI to a target PE' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

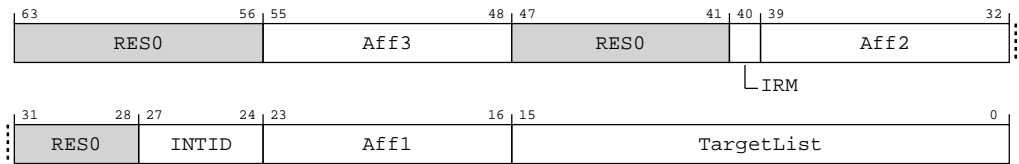
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-341: AARCH64\_ICC\_SGI1R\_EL1 bit assignments



**Table A-864: ICC\_SGI1R\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:48]	Aff3	The affinity 3 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 {x}
[47:41]	RES0	Reserved	RES0
[40]	IRM	Interrupt Routing Mode. Determines how the generated interrupts are distributed to PEs. Possible values are:  <b>0b0</b> Interrupts routed to the PEs specified by Aff3.Aff2.Aff1.<target list>.  <b>0b1</b> Interrupts routed to all PEs in the system, excluding "self".	x
[39:32]	Aff2	The affinity 2 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 {x}
[31:28]	RES0	Reserved	RES0
[27:24]	INTID	The INTID of the SGI.	xxxx
[23:16]	Aff1	The affinity 1 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 {x}
[15:0]	TargetList	Target List. The set of PEs for which SGI interrupts will be generated. Each bit corresponds to the PE within a cluster with an Affinity 0 value equal to the bit number.  If a bit is 1 and the bit does not correspond to a valid target PE, the bit must be ignored by the Distributor. It is IMPLEMENTATION DEFINED whether, in such cases, a Distributor can signal a system error.  If the IRM bit is 1, this field is <b>RES0</b> .	16 {x}

## Access

MSR ICC\_SGI1R\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b101

## Accessibility

MSR ICC\_SGI1R\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ICC_SGI1R_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        ICC_SGI1R_EL1 = X[t, 64];

```

A.2.6.19 ICC\_ASGI1R\_EL1, Interrupt Controller Alias Software Generated Interrupt Group 1 Register

Generates Group 1 SGIs for the Security state that is not the current Security state.

Configurations

Under certain conditions a write to ICC\_ASGI1R\_EL1 can generate Group 0 interrupts, see 'Forwarding an SGI to a target PE' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

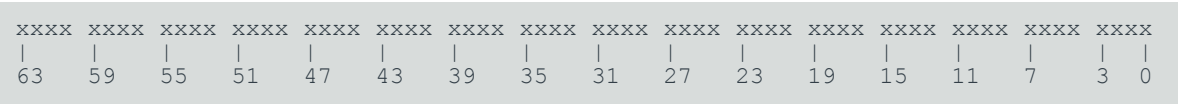
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-342: AARCH64\_ICC\_ASGI1R\_EL1 bit assignments

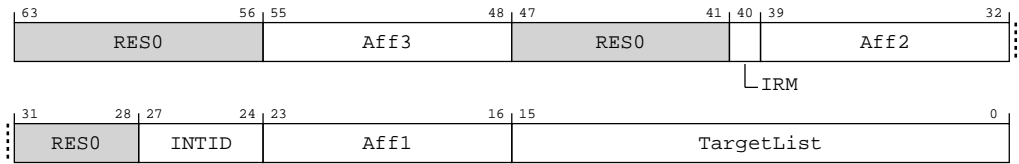


Table A-866: ICC\_ASGI1R\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:48]	Aff3	The affinity 3 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is RES0.	8 { x }

Bits	Name	Description	Reset
[47:41]	<b>RES0</b>	Reserved	<b>RES0</b>
[40]	IRM	Interrupt Routing Mode. Determines how the generated interrupts are distributed to PEs. Possible values are:  <b>0b0</b> Interrupts routed to the PEs specified by Aff3.Aff2.Aff1.<target list>.  <b>0b1</b> Interrupts routed to all PEs in the system, excluding "self".	x
[39:32]	Aff2	The affinity 2 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 {x}
[31:28]	<b>RES0</b>	Reserved	<b>RES0</b>
[27:24]	INTID	The INTID of the SGI.	xxxx
[23:16]	Aff1	The affinity 1 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 {x}
[15:0]	TargetList	Target List. The set of PEs for which SGI interrupts will be generated. Each bit corresponds to the PE within a cluster with an Affinity 0 value equal to the bit number.  If a bit is 1 and the bit does not correspond to a valid target PE, the bit must be ignored by the Distributor. It is IMPLEMENTATION DEFINED whether, in such cases, a Distributor can signal a system error.  If the IRM bit is 1, this field is <b>RES0</b> .	16 {x}

## Access

This register allows software executing in a Secure state to generate Non-secure Group 1 SGIs.

MSR ICC\_ASGI1R\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b110

## Accessibility

This register allows software executing in a Secure state to generate Non-secure Group 1 SGIs.

MSR ICC\_ASGI1R\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ICC_ASGI1R_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        ICC_ASGI1R_EL1 = X[t, 64];

```

A.2.6.20 ICC\_SGI0R\_EL1, Interrupt Controller Software Generated Interrupt Group 0 Register

Generates Secure Group 0 SGIs.

Configurations

This register is available in all configurations.

Attributes

Width

64

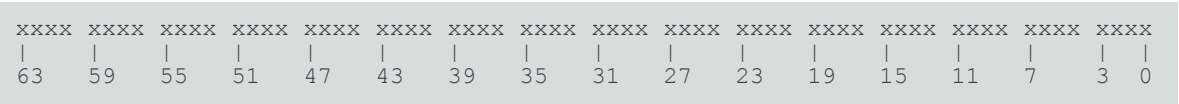
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-343: AARCH64\_ICC\_SGI0R\_EL1 bit assignments

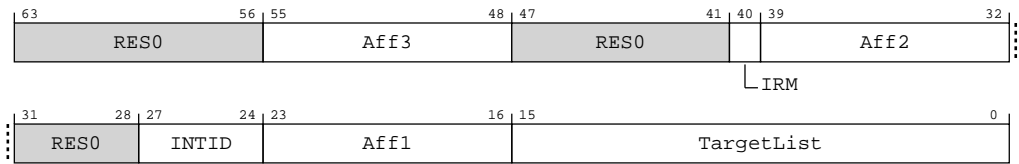


Table A-868: ICC\_SGI0R\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:48]	Aff3	The affinity 3 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is RES0.	8 {x}
[47:41]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[40]	IRM	Interrupt Routing Mode. Determines how the generated interrupts are distributed to PEs. Possible values are:  <b>0b0</b> Interrupts routed to the PEs specified by Aff3.Aff2.Aff1.<target list>.  <b>0b1</b> Interrupts routed to all PEs in the system, excluding "self".	<b>x</b>
[39:32]	Aff2	The affinity 2 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 { <b>x</b> }
[31:28]	<b>RES0</b>	Reserved	<b>RES0</b>
[27:24]	INTID	The INTID of the SGI.	<b>xxxx</b>
[23:16]	Aff1	The affinity 1 value of the affinity path of the cluster for which SGI interrupts will be generated.  If the IRM bit is 1, this field is <b>RES0</b> .	8 { <b>x</b> }
[15:0]	TargetList	Target List. The set of PEs for which SGI interrupts will be generated. Each bit corresponds to the PE within a cluster with an Affinity 0 value equal to the bit number.  If a bit is 1 and the bit does not correspond to a valid target PE, the bit must be ignored by the Distributor. It is IMPLEMENTATION DEFINED whether, in such cases, a Distributor can signal a system error.  If the IRM bit is 1, this field is <b>RES0</b> .	16 { <b>x</b> }

## Access

This register allows software executing in a Secure state to generate Group 0 SGIs. It will also allow software executing in a Non-secure state to generate Group 0 SGIs, if permitted by the settings of ext-GICR\_NSACR in the Redistributor corresponding to the target PE.

When ext-GICD\_CTLR.DS==0, Non-secure writes do not generate an interrupt for a target PE if not permitted by the ext-GICR\_NSACR register associated with the target PE. For more information, see 'Use of control registers for SGI forwarding' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

MSR ICC\_SGIOR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1011	0b111

## Accessibility

This register allows software executing in a Secure state to generate Group 0 SGIs. It will also allow software executing in a Non-secure state to generate Group 0 SGIs, if permitted by the settings of ext-GICR\_NSACR in the Redistributor corresponding to the target PE.

When ext-GICD\_CTLR.DS==0, Non-secure writes do not generate an interrupt for a target PE if not permitted by the ext-GICR\_NSACR register associated with the target PE. For more information, see 'Use of control registers for SGI forwarding' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

## MSR ICC\_SGIOR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ICC_SGIOR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_SGIOR_EL1 = X[t, 64];

```

## A.2.6.21 ICC\_IAR1\_EL1, Interrupt Controller Interrupt Acknowledge Register 1

The PE reads this register to obtain the INTID of the signaled Group 1 interrupt. This read acts as an acknowledge for the interrupt.

**Configurations**

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that reads of this register are self-synchronising when interrupts are masked by the PE (that is when  $PSTATE.\{I,F\} == \{0,0\}$ ). This ensures that the effect of activating an interrupt on the signaling of interrupt exceptions is observed when a read of this register is architecturally executed so that no spurious interrupt exception occurs if interrupts are unmasked by an instruction immediately following the read. For more information, see 'Observability of the effects of accesses to the GIC registers' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

**Attributes****Width**

64

**Functional group**

GIC system registers

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-344: AARCH64\_ICC\_IAR1\_EL1 bit assignments

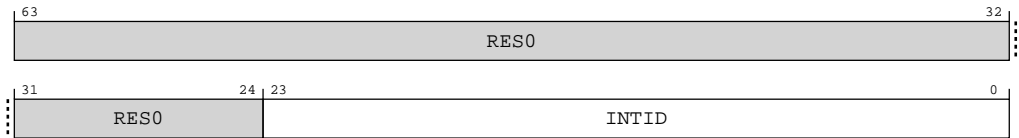


Table A-870: ICC\_IAR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	<p>The INTID of the signaled interrupt.</p> <p>This is the INTID of the highest priority pending interrupt, if that interrupt is of sufficient priority for it to be signaled to the PE, and if it can be acknowledged at the current Security state and Exception level.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are RES0.</p>	24 {x}

Access

MRS <Xt>, ICC\_IAR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b000

Accessibility

MRS <Xt>, ICC\_IAR1\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_IAR1_EL1;
    else
        X[t, 64] = ICC_IAR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_IAR1_EL1;
```

A.2.6.22 ICV\_IAR1\_EL1, Interrupt Controller Virtual Interrupt Acknowledge Register 1

The PE reads this register to obtain the INTID of the signaled virtual Group 1 interrupt. This read acts as an acknowledge for the interrupt.

Configurations

To allow software to ensure appropriate observability of actions initiated by GIC register accesses, the PE and CPU interface logic must ensure that reads of this register are self-synchronising when interrupts are masked by the PE (that is when PSTATE.{I,F} == {0,0}). This ensures that the effect of activating an interrupt on the signaling of interrupt exceptions is observed when a read of this register is architecturally executed so that no spurious interrupt exception occurs if interrupts are unmasked by an instruction immediately following the read. For more information, see 'Observability of the effects of accesses to the GIC registers' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0

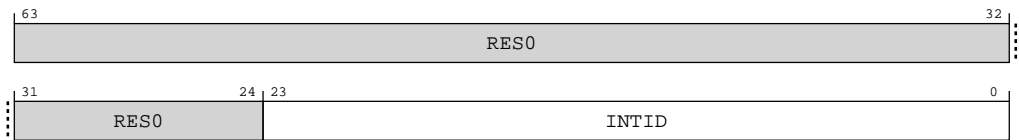


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-345: AARCH64\_ICV\_IAR1\_EL1 bit assignments



**Table A-872: ICV\_IAR1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:0]	<b>INTID</b>	<p>The INTID of the signaled virtual interrupt.</p> <p>This is the INTID of the highest priority pending virtual interrupt, if that interrupt is of sufficient priority for it to be signaled to the PE, and if it can be acknowledged.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p>	24 {x}

### Access

MRS &lt;Xt&gt;, ICC\_IAR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b000

### Accessibility

MRS &lt;Xt&gt;, ICC\_IAR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_IAR1_EL1;
    else
        X[t, 64] = ICC_IAR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_IAR1_EL1;

```

## A.2.6.23 ICC\_EOIR1\_EL1, Interrupt Controller End Of Interrupt Register 1

A PE writes to this register to inform the CPU interface that it has completed the processing of the specified Group 1 interrupt.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

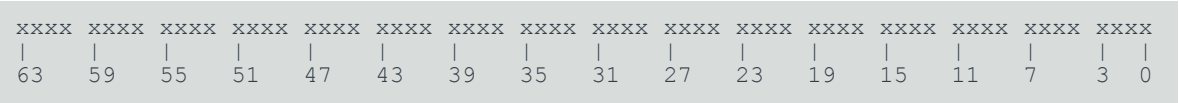
#### Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-346: AARCH64\_ICC\_EOIR1\_EL1 bit assignments

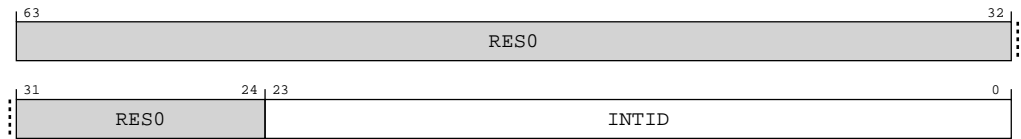


Table A-874: ICC\_EOIR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	The INTID from the corresponding AArch64-ICC_IAR1_EL1 access.  Bits [23:16] of this register are RES0.  If AArch64-ICC_CTLR_EL1.EOIMode is 0, a write to this register drops the priority for the interrupt, and also deactivates the interrupt.  If AArch64-ICC_CTLR_EL1.EOIMode is 1, a write to this register only drops the priority for the interrupt and software must write to AArch64-ICC_DIR_EL1 to deactivate the interrupt.	24 {x}

Access

A write to this register must correspond to the most recent valid read by this PE from an Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICC\_IAR1\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

A write of a Special INTID is ignored. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

MSR ICC\_EOIR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b001

### Accessibility

A write to this register must correspond to the most recent valid read by this PE from an Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICC\_IAR1\_EL1, otherwise the system behavior is UNPREDICTABLE. A valid read is a read that returns a valid INTID that is not a special INTID.

A write of a Special INTID is ignored. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

MSR ICC\_EOIR1\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        ICV_EOIR1_EL1 = X[t, 64];
    else
        ICC_EOIR1_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        ICC_EOIR1_EL1 = X[t, 64];

```

#### A.2.6.24 ICV\_EOIR1\_EL1, Interrupt Controller Virtual End Of Interrupt Register 1

A PE writes to this register to inform the CPU interface that it has completed the processing of the specified virtual Group 1 interrupt.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

GIC system registers

#### Access type

See bit descriptions

#### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-347: AARCH64\_ICV\_EOIR1\_EL1 bit assignments

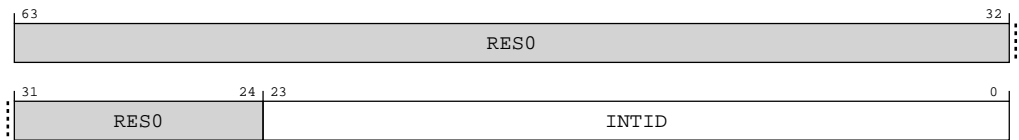


Table A-876: ICV\_EOIR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	The INTID from the corresponding AArch64-ICV_IAR1_EL1 access.  Bits [23:16] of this register are <b>RES0</b> .  If the AArch64-ICV_CTLR_EL1.EOImode bit is 0, a write to this register drops the priority for the virtual interrupt, and also deactivates the virtual interrupt.  If the AArch64-ICV_CTLR_EL1.EOImode bit is 1, a write to this register only drops the priority for the virtual interrupt. Software must write to AArch64-ICV_DIR_EL1 to deactivate the virtual interrupt.	24 {x}

Access

A write to this register must correspond to the most recent valid read by this vPE from a Virtual Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICV\_IAR1\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

MSR ICC\_EOIR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b001

Accessibility

A write to this register must correspond to the most recent valid read by this vPE from a Virtual Interrupt Acknowledge Register, and must correspond to the INTID that was read from AArch64-ICV\_IAR1\_EL1, otherwise the system behavior is **UNPREDICTABLE**. A valid read is a read that returns a valid INTID that is not a special INTID.

MSR ICC\_EOIR1\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
  if ICH_HCR_EL2.TALL1 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  elseif HCR_EL2.IMO == '1' then
    ICV_EOIR1_EL1 = X[t, 64];
  else
    ICC_EOIR1_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
  ICC_EOIR1_EL1 = X[t, 64];
```

A.2.6.25 ICC\_HPPIR1\_EL1, Interrupt Controller Highest Priority Pending Interrupt Register 1

Indicates the highest priority pending Group 1 interrupt on the CPU interface.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

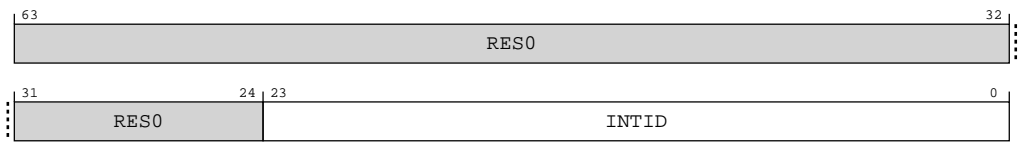


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-348: AARCH64\_ICC\_HPPIR1\_EL1 bit assignments



**Table A-878: ICC\_HPPIR1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:0]	INTID	<p>The INTID of the highest priority pending interrupt, if that interrupt is observable at the current Security state and Exception level.</p> <p>If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. These special INTIDs can be one of: 1020, 1021, or 1023. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>Bits [23:16] of this register are <b>RES0</b>.</p>	24 {x}

### Access

MRS &lt;Xt&gt;, ICC\_HPPIR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b010

### Accessibility

MRS &lt;Xt&gt;, ICC\_HPPIR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_HPPIR1_EL1;
    else
        X[t, 64] = ICC_HPPIR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_HPPIR1_EL1;

```

## A.2.6.26 ICV\_HPPIR1\_EL1, Interrupt Controller Virtual Highest Priority Pending Interrupt Register 1

Indicates the highest priority pending virtual Group 1 interrupt on the virtual CPU interface.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

#### Functional group

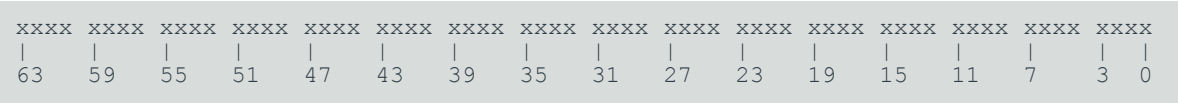
GIC system registers



Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-349: AARCH64\_ICV\_HPPIR1\_EL1 bit assignments

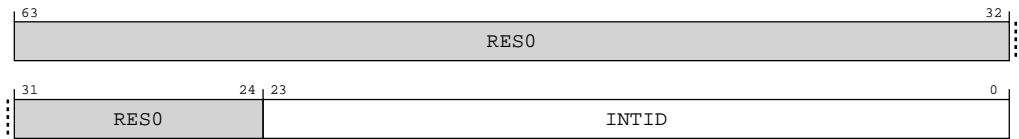


Table A-880: ICV\_HPPIR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0
[23:0]	INTID	The INTID of the highest priority pending virtual interrupt.  If the highest priority pending interrupt is not observable, this field contains a special INTID to indicate the reason. This special INTID can take the value 1023 only. For more information, see 'Special INTIDs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).  Bits [23:16] of this register are RES0.	24 {x}

Access

MRS <Xt>, ICC\_HPPIR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b010

Accessibility

MRS <Xt>, ICC\_HPPIR1\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
```

```
elseif HCR_EL2.IMO == '1' then
    X[t, 64] = ICV_HPPIR1_EL1;
else
    X[t, 64] = ICC_HPPIR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_HPPIR1_EL1;
```

A.2.6.27 ICC\_BPR1\_EL1, Interrupt Controller Binary Point Register 1

Defines the point at which the priority value fields split into two parts, the group priority field and the subpriority field. The group priority field determines Group 1 interrupt preemption.

Configurations

Virtual accesses to this register update AArch64-ICH\_VMCR\_EL2.VBPR1.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-350: AARCH64\_ICC\_BPR1\_EL1 bit assignments

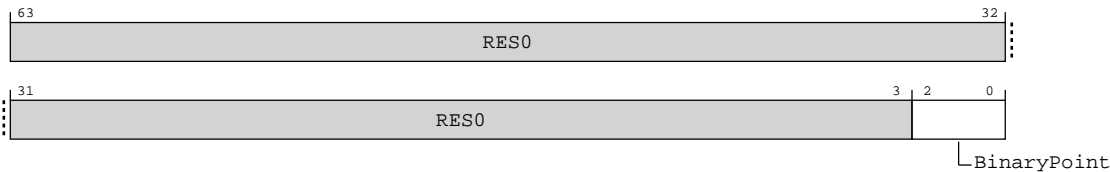


Table A-882: ICC\_BPR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2:0]	BinaryPoint	If the GIC is configured to use separate binary point fields for Group 0 and Group 1 interrupts, the value of this field controls how the 8-bit interrupt priority field is split into a group priority field, that determines interrupt preemption, and a subpriority field. For more information about priorities, see 'Priority grouping' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).  The minimum value of the Secure copy of this register is the minimum value of AArch64-ICC_BPR0_EL1.	xxx

## Access

On a reset, the binary point field is **UNKNOWN**.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value.

MRS <Xt>, ICC\_BPR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b011

MSR ICC\_BPR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b011

## Accessibility

On a reset, the binary point field is **UNKNOWN**.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value.

MRS <Xt>, ICC\_BPR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICC_BPR1_EL1;
    else
        X[t, 64] = ICC_BPR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_BPR1_EL1;

```

MSR ICC\_BPR1\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        ICC_BPR1_EL1 = X[t, 64];

```

```
else
    ICC_BPR1_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_BPR1_EL1 = X[t, 64];
```

A.2.6.28 ICV\_BPR1\_EL1, Interrupt Controller Virtual Binary Point Register 1

Defines the point at which the priority value fields split into two parts, the group priority field and the subpriority field. The group priority field determines virtual Group 1 interrupt preemption.

Configurations

This register is available in all configurations.

Attributes

Width

64

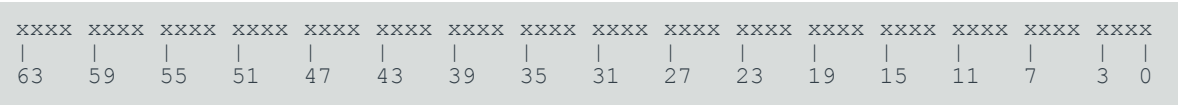
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-351: AARCH64\_ICV\_BPR1\_EL1 bit assignments

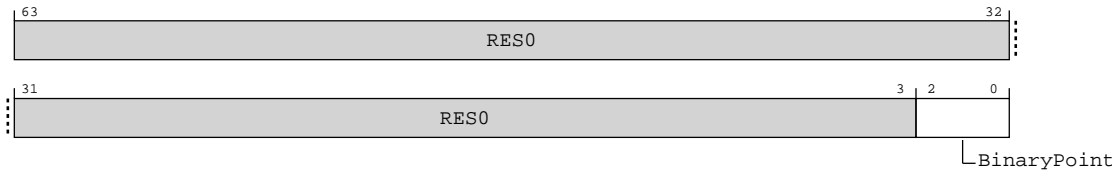


Table A-885: ICV\_BPR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2:0]	BinaryPoint	<p>If the GIC is configured to use separate binary point fields for Group 0 and Group 1 interrupts, the value of this field controls how the 8-bit interrupt priority field is split into a group priority field, that determines interrupt preemption, and a subpriority field.</p> <p>For more information about priorities, see 'Priority grouping' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).</p> <p>An attempt to program this field to a value less than the minimum value sets the field to the minimum value.</p> <p>If AArch64-ICV_CTLR_EL1.CBPR is set to 1, Secure EL1 reads return AArch64-ICV_BPR0_EL1. Secure EL1 writes modify AArch64-ICV_BPR0_EL1.</p>	xxx

## Access

For Secure writes, the minimum value of this field is the minimum value of AArch64-ICH\_VMCR\_EL2.VBPR0.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value. On a reset, the binary point field is **UNKNOWN**.

MRS <Xt>, ICC\_BPR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b011

MSR ICC\_BPR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b011

## Accessibility

For Secure writes, the minimum value of this field is the minimum value of AArch64-ICH\_VMCR\_EL2.VBPR0.

An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value. On a reset, the binary point field is UNKNOWN.

MRS <Xt>, ICC\_BPR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_BPR1_EL1;
    else
        X[t, 64] = ICC_BPR1_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_BPR1_EL1;

```

MSR ICC\_BPR1\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        ICV_BPR1_EL1 = X[t, 64];
    else
        ICC_BPR1_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_BPR1_EL1 = X[t, 64];
```

A.2.6.29 ICC\_CTLR\_EL1, Interrupt Controller Control Register (EL1)

Controls aspects of the behavior of the GIC CPU interface and provides information about the features implemented.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	10xx	1000	0100	x0xx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-352: AARCH64\_ICC\_CTLR\_EL1 bit assignments

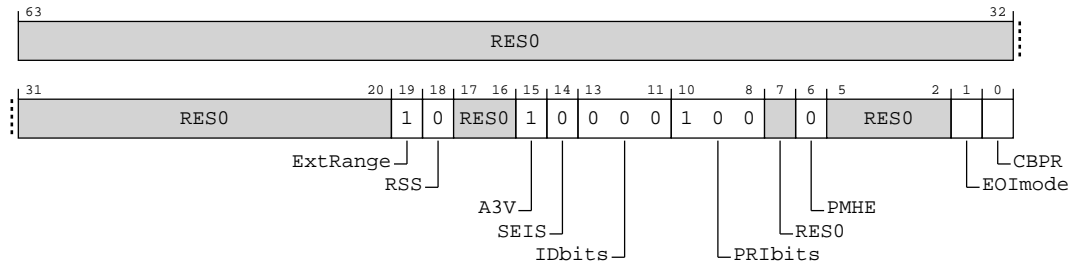


Table A-888: ICC\_CTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0
[19]	ExtRange	Extended INTID range (read-only). <b>0b1</b> CPU interface supports INTIDs in the range 1024..8191 <ul style="list-style-type: none"> <li>All INTIDs in the range 1024..8191 are treated as requiring deactivation.</li> </ul>	0b1
[18]	RSS	Range Selector Support. Possible values are: <b>0b0</b> Targeted SGLs with affinity level 0 values of 0 - 15 are supported.  This bit is read-only.	0b0
[17:16]	RES0	Reserved	RES0
[15]	A3V	Affinity 3 Valid. Read-only and writes are ignored. Possible values are: <b>0b1</b> The CPU interface logic supports nonzero values of Affinity 3 in SGL generation System registers.	0b1
[14]	SEIS	SEI Support. Read-only and writes are ignored. Indicates whether the CPU interface supports local generation of SEIs: <b>0b0</b> The CPU interface logic does not support local generation of SEIs.	0b0
[13:11]	IDbits	Identifier bits. Read-only and writes are ignored. The number of physical interrupt identifier bits supported: <b>0b000</b> 16 bits.  All other values are reserved.	0b000
[10:8]	PRIbits	Priority bits. Read-only and writes are ignored. The number of priority bits implemented, minus one.  For physical accesses, this field determines the minimum value of AArch64-ICC_BPR0_EL1.  Physical accesses return the value from this field. <b>0b100</b> 5 bits of priority are implemented	0b100
[7]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[6]	PMHE	Priority Mask Hint Enable. Controls whether the priority mask register is used as a hint for interrupt distribution:  <b>0b0</b> Disables use of AArch64-ICC_PMR_EL1 as a hint for interrupt distribution.  Read-only and writes are ignored.	0b0
[5:2]	RES0	Reserved	RES0
[1]	EOImode	EOI mode for the current Security state. Controls whether a write to an End of Interrupt register also deactivates the interrupt:  <b>0b0</b> AArch64-ICC_EOIR0_EL1 and AArch64-ICC_EOIR1_EL1 provide both priority drop and interrupt deactivation functionality. Accesses to AArch64-ICC_DIR_EL1 are <b>UNPREDICTABLE</b> .  <b>0b1</b> AArch64-ICC_EOIR0_EL1 and AArch64-ICC_EOIR1_EL1 provide priority drop functionality only. AArch64-ICC_DIR_EL1 provides interrupt deactivation functionality.	x
[0]	CBPR	Common Binary Point Register. Controls whether the same register is used for interrupt preemption of both Group 0 and Group 1 interrupts:  <b>0b0</b> AArch64-ICC_BPRO_EL1 determines the preemption group for Group 0 interrupts only.  AArch64-ICC_BPR1_EL1 determines the preemption group for Group 1 interrupts.  <b>0b1</b> AArch64-ICC_BPRO_EL1 determines the preemption group for both Group 0 and Group 1 interrupts.	x

## Access

MRS <Xt>, ICC\_CTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b100

MSR ICC\_CTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b100

## Accessibility

MRS <Xt>, ICC\_CTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_CTLR_EL1;
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_CTLR_EL1;
    else
        X[t, 64] = ICC_CTLR_EL1;

```



```
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_CTLR_EL1;
```

MSR ICC\_CTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_CTLR_EL1 = X[t, 64];
    elseif HCR_EL2.IMO == '1' then
        ICV_CTLR_EL1 = X[t, 64];
    else
        ICC_CTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_CTLR_EL1 = X[t, 64];
```

A.2.6.30 ICV\_CTLR\_EL1, Interrupt Controller Virtual Control Register

Controls aspects of the behavior of the GIC virtual CPU interface and provides information about the features implemented.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	10xx	1000	0100	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-353: AARCH64\_ICV\_CTLR\_EL1 bit assignments

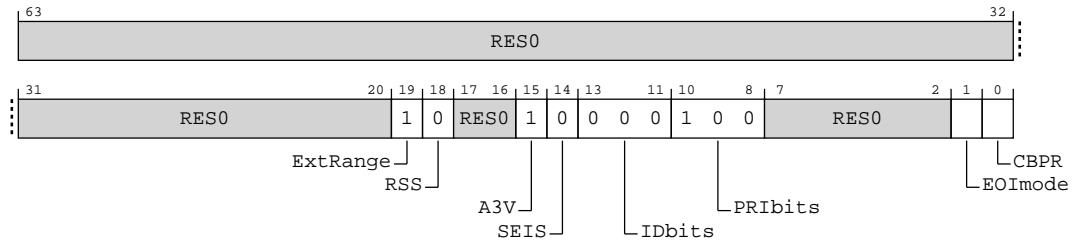


Table A-891: ICV\_CTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0
[19]	ExtRange	Extended INTID range (read-only).  <b>0b1</b> CPU interface supports INTIDs in the range 1024..8191 <ul style="list-style-type: none"> <li>All INTIDs in the range 1024..8191 are treated as requiring deactivation.</li> </ul> ICV_CTLR_EL1.ExtRange is an alias of AArch64-ICC_CTLR_EL1.ExtRange.	0b1
[18]	RSS	Range Selector Support. Possible values are:  <b>0b0</b> Targeted SGIs with affinity level 0 values of 0 - 15 are supported.  This bit is read-only.	0b0
[17:16]	RES0	Reserved	RES0
[15]	A3V	Affinity 3 Valid. Read-only and writes are ignored. Possible values are:  <b>0b1</b> The virtual CPU interface logic supports nonzero values of Affinity 3 in SGI generation System registers.	0b1
[14]	SEIS	SEI Support. Read-only and writes are ignored. Indicates whether the virtual CPU interface supports local generation of SEIs:  <b>0b0</b> The virtual CPU interface logic does not support local generation of SEIs.	0b0
[13:11]	IDbits	Identifier bits. Read-only and writes are ignored. The number of virtual interrupt identifier bits supported:  <b>0b000</b> 16 bits.  All other values are reserved.	0b000

Bits	Name	Description	Reset
[10:8]	PRIbits	<p>Priority bits. Read-only and writes are ignored. The number of priority bits implemented, minus one.</p> <p>An implementation must implement at least 32 levels of physical priority (5 priority bits).</p> <p><b>Note:</b> This field always returns the number of priority bits implemented.</p> <p>The division between group priority and subpriority is defined in the binary point registers AArch64-ICV_BPR0_EL1 and AArch64-ICV_BPR1_EL1.</p> <p><b>0b100</b> 5 bits of priority are implemented</p>	0b100
[7:2]	RES0	Reserved	RES0
[1]	EOImode	<p>Virtual EOI mode. Controls whether a write to an End of Interrupt register also deactivates the virtual interrupt:</p> <p><b>0b0</b> AArch64-ICV_EOIR0_EL1 and AArch64-ICV_EOIR1_EL1 provide both priority drop and interrupt deactivation functionality. Accesses to AArch64-ICV_DIR_EL1 are <b>UNPREDICTABLE</b>.</p> <p><b>0b1</b> AArch64-ICV_EOIR0_EL1 and AArch64-ICV_EOIR1_EL1 provide priority drop functionality only. AArch64-ICV_DIR_EL1 provides interrupt deactivation functionality.</p>	x
[0]	CBPR	<p>Common Binary Point Register. Controls whether the same register is used for interrupt preemption of both virtual Group 0 and virtual Group 1 interrupts:</p> <p><b>0b0</b> AArch64-ICV_BPR1_EL1 determines the preemption group for virtual Group 1 interrupts.</p> <p><b>0b1</b> Secure reads of AArch64-ICV_BPR1_EL1 return AArch64-ICV_BPR0_EL1. Secure writes of AArch64-ICV_BPR1_EL1 modify AArch64-ICV_BPR0_EL1.</p>	x

## Access

MRS <Xt>, ICC\_CTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b100

MSR ICC\_CTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b100

## Accessibility

MRS <Xt>, ICC\_CTLR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then

```

```
        X[t, 64] = ICV_CTLR_EL1;
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_CTLR_EL1;
    else
        X[t, 64] = ICC_CTLR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_CTLR_EL1;
```

MSR ICC\_CTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TC == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        ICV_CTLR_EL1 = X[t, 64];
    elsif HCR_EL2.IMO == '1' then
        ICV_CTLR_EL1 = X[t, 64];
    else
        ICC_CTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ICC_CTLR_EL1 = X[t, 64];
```

A.2.6.31 ICC\_SRE\_EL1, Interrupt Controller System Register Enable Register (EL1)

Controls whether the System register interface or the memory-mapped interface to the GIC CPU interface is used for EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-354: AARCH64\_ICC\_SRE\_EL1 bit assignments

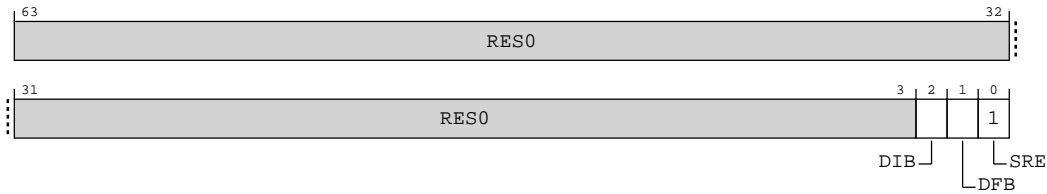


Table A-894: ICC\_SRE\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0
[2]	DIB	Disable IRQ bypass.  <b>0b0</b> IRQ bypass enabled.  <b>0b1</b> IRQ bypass disabled.  This field is a read-only alias of AArch64-ICC_SRE_EL2.DIB.	0b0
[1]	DFB	Disable FIQ bypass.  <b>0b0</b> FIQ bypass enabled.  <b>0b1</b> FIQ bypass disabled.  This field is a read-only alias of AArch64-ICC_SRE_EL2.DFB.	0b0
[0]	SRE	System Register Enable.  <b>0b1</b> The System register interface for the current Security state is enabled.	0b1

Access

Execution with AArch64-ICC\_SRE\_EL1.SRE set to 0 might make some System registers **UNKNOWN**.

MRS <Xt>, ICC\_SRE\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b101

MSR ICC\_SRE\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b101

Accessibility

Execution with AArch64-ICC\_SRE\_EL1.SRE set to 0 might make some System registers UNKNOWN.

MRS <Xt>, ICC\_SRE\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = ICC_SRE_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_SRE_EL1;
```

MSR ICC\_SRE\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    ICC_SRE_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_SRE_EL1 = X[t, 64];
```

A.2.6.32 ICC\_IGRPEN0\_EL1, Interrupt Controller Interrupt Group 0 Enable register

Controls whether Group 0 interrupts are enabled or not.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-355: AARCH64\_ICC\_IGRPEN0\_EL1 bit assignments

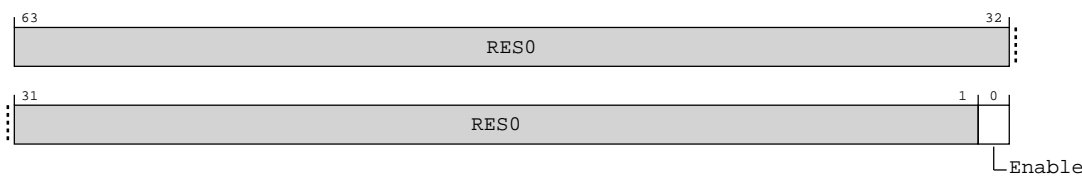


Table A-897: ICC\_IGRPEN0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	Enable	Enables Group 0 interrupts.  <b>0b0</b> Group 0 interrupts are disabled.  <b>0b1</b> Group 0 interrupts are enabled.  Virtual accesses to this register update AArch64-ICH_VMCR_EL2.VENG0.  If the highest priority pending interrupt for that PE is a Group 0 interrupt using 1 of N model, then the interrupt will be targeted to another PE as a result of the Enable bit changing from 1 to 0.	0b0

Access

MRS <Xt>, ICC\_IGRPEN0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b110

MSR ICC\_IGRPEN0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b110

Accessibility

MRS <Xt>, ICC\_IGRPEN0\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_IGRPEN0_EL1;
    else
        X[t, 64] = ICC_IGRPEN0_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_IGRPEN0_EL1;
```

MSR ICC\_IGRPEN0\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        ICV_IGRPEN0_EL1 = X[t, 64];
    else
        ICC_IGRPEN0_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ICC_IGRPEN0_EL1 = X[t, 64];
```

A.2.6.33 ICV\_IGRPEN0\_EL1, Interrupt Controller Virtual Interrupt Group 0 Enable register

Controls whether virtual Group 0 interrupts are enabled or not.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-356: AARCH64\_ICV\_IGRPEN0\_EL1 bit assignments

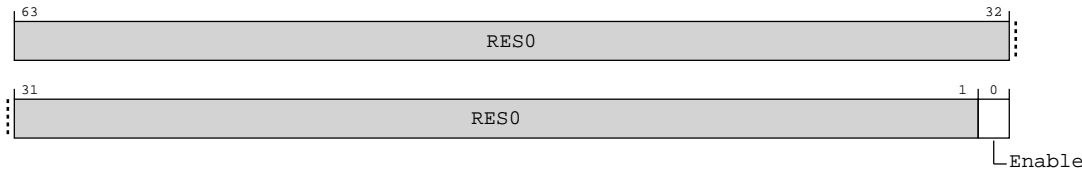


Table A-900: ICV\_IGRPEN0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	Enable	Enables virtual Group 0 interrupts.  <b>0b0</b> Virtual Group 0 interrupts are disabled.  <b>0b1</b> Virtual Group 0 interrupts are enabled.	x

Access

MRS <Xt>, ICC\_IGRPEN0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b110

MSR ICC\_IGRPEN0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b110

Accessibility

MRS <Xt>, ICC\_IGRPEN0\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL0 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.FMO == '1' then
        X[t, 64] = ICV_IGRPEN0_EL1;
    else
        X[t, 64] = ICC_IGRPEN0_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_IGRPEN0_EL1;
```

MSR ICC\_IGRPEN0\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
  if ICH_HCR_EL2.TALL0 == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  elseif HCR_EL2.FMO == '1' then
    ICV_IGRPEN0_EL1 = X[t, 64];
  else
    ICC_IGRPEN0_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
  ICC_IGRPEN0_EL1 = X[t, 64];
```

A.2.6.34 ICC\_IGRPEN1\_EL1, Interrupt Controller Interrupt Group 1 Enable register

Controls whether Group 1 interrupts are enabled for the current Security state.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

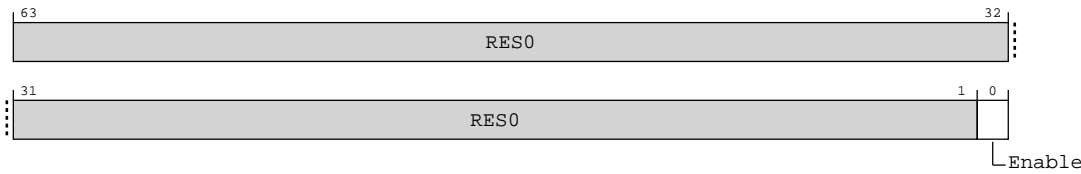
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-357: AARCH64\_ICC\_IGRPEN1\_EL1 bit assignments



**Table A-903: ICC\_IGRPEN1\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	Enable	<p>Enables Group 1 interrupts for the current Security state.</p> <p><b>0b0</b></p> <p>Group 1 interrupts are disabled for the current Security state.</p> <p><b>0b1</b></p> <p>Group 1 interrupts are enabled for the current Security state.</p> <p>Virtual accesses to this register update AArch64-ICH_VMCR_EL2.VENG1.</p> <p>If the highest priority pending interrupt for that PE is a Group 1 interrupt using 1 of N model, then the interrupt will target another PE as a result of the Enable bit changing from 1 to 0.</p>	0b0

### Access

MRS &lt;Xt&gt;, ICC\_IGRPEN1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b111

MSR ICC\_IGRPEN1\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b111

### Accessibility

MRS &lt;Xt&gt;, ICC\_IGRPEN1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_IGRPEN1_EL1;
    else
        X[t, 64] = ICC_IGRPEN1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICC_IGRPEN1_EL1;

```

MSR ICC\_IGRPEN1\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elseif HCR_EL2.IMO == '1' then
        ICV_IGRPEN1_EL1 = X[t, 64];
    else
        ICC_IGRPEN1_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then

```

```
ICC_IGRPEN1_EL1 = X[t, 64];
```

A.2.6.35 ICV\_IGRPEN1\_EL1, Interrupt Controller Virtual Interrupt Group 1 Enable register

Controls whether virtual Group 1 interrupts are enabled for the current Security state.

Configurations

This register is available in all configurations.

Attributes

Width

64

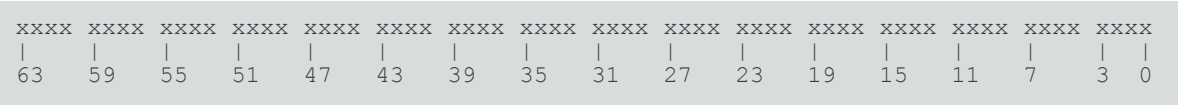
Functional group

GIC system registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-358: AARCH64\_ICV\_IGRPEN1\_EL1 bit assignments

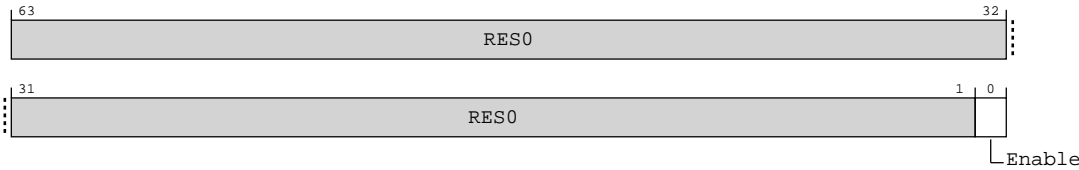


Table A-906: ICV\_IGRPEN1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	Enable	Enables virtual Group 1 interrupts.  <b>0b0</b> Virtual Group 1 interrupts are disabled.  <b>0b1</b> Virtual Group 1 interrupts are enabled.	x

### Access

MRS <Xt>, ICC\_IGRPEN1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b111

MSR ICC\_IGRPEN1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b1100	0b111

### Accessibility

MRS <Xt>, ICC\_IGRPEN1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        X[t, 64] = ICV_IGRPEN1_EL1;
    else
        X[t, 64] = ICC_IGRPEN1_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ICC_IGRPEN1_EL1;

```

MSR ICC\_IGRPEN1\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if ICH_HCR_EL2.TALL1 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HCR_EL2.IMO == '1' then
        ICV_IGRPEN1_EL1 = X[t, 64];
    else
        ICC_IGRPEN1_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        ICC_IGRPEN1_EL1 = X[t, 64];

```

A.2.6.36 ICH\_LR<n>\_EL2, Interrupt Controller List Registers, n = 0 - 15

Provides interrupt context information for the virtual CPU interface.

Configurations

If list register n is not implemented, then accesses to this register are UNDEFINED.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-359: AARCH64\_ICH\_LR<n>\_EL2 bit assignments

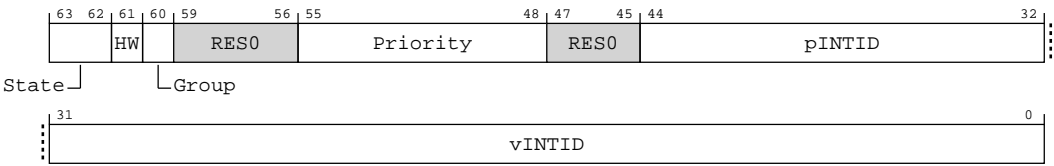


Table A-909: ICH\_LR&lt;n&gt;\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:62]	State	<p>The state of the interrupt:</p> <p><b>0b00</b> Invalid (Inactive).</p> <p><b>0b01</b> Pending.</p> <p><b>0b10</b> Active.</p> <p><b>0b11</b> Pending and active.</p> <p>The GIC updates these state bits as virtual interrupts proceed through the interrupt life cycle. Entries in the invalid state are ignored, except for the purpose of generating virtual maintenance interrupts.</p> <p>For hardware interrupts, the pending and active state is held in the physical Distributor rather than the virtual CPU interface. A hypervisor must only use the pending and active state for software originated interrupts, which are typically associated with virtual devices, or SGIs.</p>	xx
[61]	HW	<p>Indicates whether this virtual interrupt maps directly to a hardware interrupt, meaning that it corresponds to a physical interrupt. Deactivation of the virtual interrupt also causes the deactivation of the physical interrupt with the ID that the pINTID field indicates.</p> <p><b>0b0</b> The interrupt is triggered entirely by software. No notification is sent to the Distributor when the virtual interrupt is deactivated.</p> <p><b>0b1</b> The interrupt maps directly to a hardware interrupt. A deactivate interrupt request is sent to the Distributor when the virtual interrupt is deactivated, using the pINTID field from this register to indicate the physical interrupt ID.</p> <p>If AArch64-ICH_VMCR_EL2.VEOIM is 0, this request corresponds to a write to AArch64-ICC_EOIR0_EL1 or AArch64-ICC_EOIR1_EL1. Otherwise, it corresponds to a write to AArch64-ICC_DIR_EL1.</p>	x
[60]	Group	<p>Indicates the group for this virtual interrupt.</p> <p><b>0b0</b> This is a Group 0 virtual interrupt. AArch64-ICH_VMCR_EL2.VFIQEn determines whether it is signaled as a virtual IRQ or as a virtual FIQ, and AArch64-ICH_VMCR_EL2.VENG0 enables signaling of this interrupt to the virtual machine.</p> <p><b>0b1</b> This is a Group 1 virtual interrupt, signaled as a virtual IRQ. AArch64-ICH_VMCR_EL2.VENG1 enables the signalling of this interrupt to the virtual machine.</p> <p>If AArch64-ICH_VMCR_EL2.VCBPR is 0, then AArch64-ICC_BPR1_EL1 determines if a pending Group 1 interrupt has sufficient priority to preempt current execution. Otherwise, AArch64-ICH_LR&lt;n&gt;_EL2 determines preemption.</p>	x
[59:56]	RES0	Reserved	RES0
[55:48]	Priority	The priority of this interrupt. Bits [50:48] are <b>RES0</b> .	8 {x}
[47:45]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[44:32]	pINTID	<p>Physical INTID, for hardware interrupts.</p> <p>When ICH_LR&lt;n&gt;_EL2.HW is 0 (there is no corresponding physical interrupt), this field has the following meaning:</p> <ul style="list-style-type: none"> <li>Bits[44:42] : <b>RES0</b>.</li> <li>Bit[41] : EOI. If this bit is 1, then when the interrupt identified by vINTID is deactivated, a maintenance interrupt is asserted.</li> <li>Bits[40:32] : <b>RES0</b>.</li> </ul> <p>When ICH_LR&lt;n&gt;_EL2.HW is 1 (there is a corresponding physical interrupt):</p> <ul style="list-style-type: none"> <li>This field indicates the physical INTID. This field is only required to implement enough bits to hold a valid value for the implemented INTID size. Any unused higher order bits are <b>RES0</b>.</li> <li>When AArch64-ICC_CTLR_EL1.ExtRange is 0, then bits[44:42] of this field are <b>RES0</b>.</li> <li>If the value of pINTID is not a valid INTID, behavior is UNPREDICTABLE. If the value of pINTID indicates a PPI, this field applies to the PPI associated with this same physical PE ID as the virtual CPU interface requesting the deactivation.</li> </ul> <p>A hardware physical identifier is only required in List Registers for interrupts that require deactivation. This means only 13 bits of Physical INTID are required, regardless of the number specified by AArch64-ICC_CTLR_EL1.IDbits.</p>	13 {x}
[31:0]	vINTID	<p>Virtual INTID of the interrupt.</p> <p>If the value of vINTID is 1020-1023 and ICH_LR&lt;n&gt;_EL2.State!=0b00 (Inactive), behavior is UNPREDICTABLE.</p> <p>Behavior is UNPREDICTABLE if two or more List Registers specify the same vINTID when:</p> <ul style="list-style-type: none"> <li>ICH_LR&lt;n&gt;_EL2.State == 0b01.</li> <li>ICH_LR&lt;n&gt;_EL2.State == 0b10.</li> <li>ICH_LR&lt;n&gt;_EL2.State == 0b11.</li> </ul> <p>Bits [31:16] are <b>RES0</b>.</p> <p><b>Note:</b> When a VM is using memory-mapped access to the GIC, software must ensure that the correct source PE ID is provided in bits[12:10].</p>	32 {x}

## Access

MRS <Xt>, ICH\_LR<m>\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	'110':m[3]	m[2:0]

MSR ICH\_LR<m>\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	'110':m[3]	m[2:0]



Accessibility

MRS <Xt>, ICH\_LR<m>\_EL2

```
integer m = UInt(CRm<0>:op2<2:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_LR_EL2[m];
```

MSR ICH\_LR<m>\_EL2, <Xt>

```
integer m = UInt(CRm<0>:op2<2:0>);

if m >= 4 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ICH_LR_EL2[m] = X[t, 64];
```

A.2.6.37 ICH\_APOR<n>\_EL2, Interrupt Controller Hyp Active Priorities Group 0 Registers, n = 0

Provides information about Group 0 virtual active priorities for EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

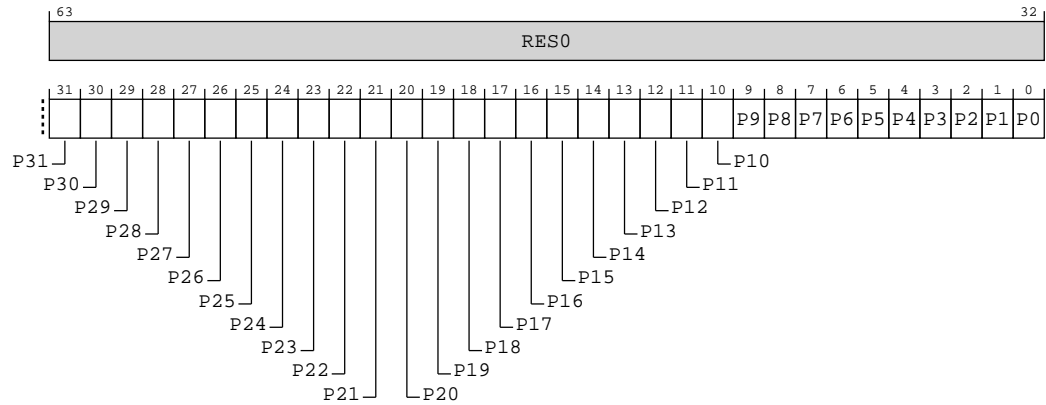
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-360: AARCH64\_ICH\_AP0R<n>\_EL2 bit assignments**



**Table A-912: ICH\_AP0R<n>\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	P<x>	<p>Provides the access to the virtual active priorities for Group 0 interrupts. Possible values of each bit are:</p> <p><b>0b0</b></p> <p>There is no Group 0 interrupt active with this priority level, or all active Group 0 interrupts with this priority level have undergone priority-drop.</p> <p><b>0b1</b></p> <p>There is a Group 0 interrupt active with this priority level which has not undergone priority drop.</p> <p>The correspondence between priority levels and bits depends on the number of bits of priority that are implemented.</p> <p>There are 32 preemption levels implemented, and the active state of these preemption levels are held in ICH_AP0R0_EL2 in the bits corresponding to Priority[7:3].</p> <p><b>Note:</b></p> <p>Having the bit corresponding to a priority set to 1 in both ICH_AP0R&lt;n&gt;_EL2 and AArch64-ICH_AP1R&lt;n&gt;_EL2 might result in <b>UNPREDICTABLE</b> behavior of the interrupt prioritization system for virtual interrupts.</p>	0x00000000

Software must ensure that ICH\_AP0R<n>\_EL2 is 0 for legacy VMs otherwise behavior is **UNPREDICTABLE**. For more information about support for legacy VMs, see 'Support for legacy operation of VMs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

The active priorities for Group 0 and Group 1 interrupts for legacy VMs are held in AArch64-ICH\_AP1R<n>\_EL2 and reads and writes to GICV\_APR access AArch64-ICH\_AP1R<n>\_EL2. This means that ICH\_AP0R<n>\_EL2 is inaccessible to legacy VMs.

## Access

ICH\_AP0R1\_EL2 is implemented only in implementations that support 6 or more bits of preemption. ICH\_AP0R2\_EL2 and ICH\_AP0R3\_EL2 are implemented only in implementations that support 7 bits of preemption. Unimplemented registers are **UNDEFINED**.



The number of bits of preemption is indicated by AArch64-ICH\_VTR\_EL2.PREbits

Writing to these registers with any value other than the last read value of the register (or 0x00000000 for a newly set up virtual machine) can result in **UNPREDICTABLE** behavior of the virtual interrupt prioritization system allowing either:

- Virtual interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution at EL1 or EL0.

Writing to the active priority registers in any order other than the following order will result in **UNPREDICTABLE** behavior:

- ICH\_AP0R<n>\_EL2.
- AArch64-ICH\_AP1R<n>\_EL2.

Having the bit corresponding to a priority set in both ICH\_AP0R<n>\_EL2 and AArch64-ICH\_AP1R<n>\_EL2 can result in **UNPREDICTABLE** behavior of the interrupt prioritization system for virtual interrupts.

MRS <Xt>, ICH\_AP0R<m>\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1000	'0':m[1:0]

MSR ICH\_AP0R<m>\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1000	'0':m[1:0]

## Accessibility

ICH\_AP0R1\_EL2 is implemented only in implementations that support 6 or more bits of preemption. ICH\_AP0R2\_EL2 and ICH\_AP0R3\_EL2 are implemented only in implementations that support 7 bits of preemption. Unimplemented registers are **UNDEFINED**.

**Note**

The number of bits of preemption is indicated by AArch64-ICH\_VTR\_EL2.PREbits

Writing to these registers with any value other than the last read value of the register (or 0x00000000 for a newly set up virtual machine) can result in UNPREDICTABLE behavior of the virtual interrupt prioritization system allowing either:

- Virtual interrupts that should preempt execution to not preempt execution.
- Interrupts that should not preempt execution to preempt execution at EL1 or EL0.

Writing to the active priority registers in any order other than the following order will result in UNPREDICTABLE behavior:

- ICH\_AP0R<n>\_EL2.
- AArch64-ICH\_AP1R<n>\_EL2.

Having the bit corresponding to a priority set in both ICH\_AP0R<n>\_EL2 and AArch64-ICH\_AP1R<n>\_EL2 can result in UNPREDICTABLE behavior of the interrupt prioritization system for virtual interrupts.

MRS <Xt>, ICH\_AP0R<m>\_EL2

```
integer m = UInt(op2<1:0>);
if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_AP0R_EL2[m];
```

MSR ICH\_AP0R<m>\_EL2, <Xt>

```
integer m = UInt(op2<1:0>);
if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ICH_AP0R_EL2[m] = X[t, 64];
```

A.2.6.38 ICH\_AP1R<n>\_EL2, Interrupt Controller Hyp Active Priorities Group 1 Registers, n = 0

Provides information about Group 1 virtual active priorities for EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

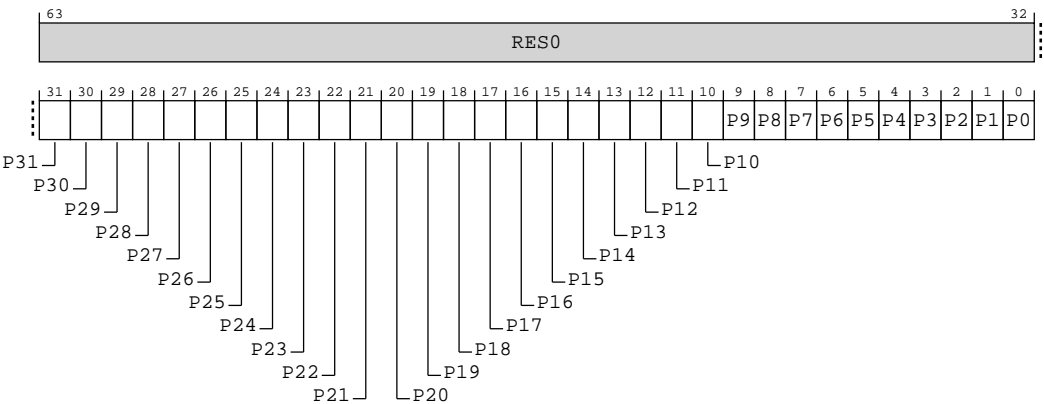
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-361: AARCH64\_ICH\_AP1R<n>\_EL2 bit assignments



**Table A-915: ICH\_AP1R<n>\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	P<x>	<p>Group 1 interrupt active priorities. Possible values of each bit are:</p> <p><b>0b0</b></p> <p>There is no Group 1 interrupt active with this priority level, or all active Group 1 interrupts with this priority level have undergone priority-drop.</p> <p><b>0b1</b></p> <p>There is a Group 1 interrupt active with this priority level which has not undergone priority drop.</p> <p>The correspondence between priority levels and bits depends on the number of bits of priority that are implemented.</p> <p>There are 32 preemption levels implemented, and the active state of these preemption levels are held in ICH_AP1R0_EL2 in the bits corresponding to Priority[7:3].</p> <p><b>Note:</b></p> <p>Having the bit corresponding to a priority set to 1 in both ICH_AP0R&lt;n&gt;_EL2 and AArch64-ICH_AP1R&lt;n&gt;_EL2 might result in <b>UNPREDICTABLE</b> behavior of the interrupt prioritization system for virtual interrupts.</p>	0x00000000

This register is always used for legacy VMs, regardless of the group of the virtual interrupt. Reads and writes to ext-GICV\_APR<n> access AArch64-ICH\_AP1R<n>\_EL2. For more information about support for legacy VMs, see 'Support for legacy operation of VMs' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069).

### Access

ICH\_AP1R1\_EL2 is implemented only in implementations that support 6 or more bits of preemption. ICH\_AP1R2\_EL2 and ICH\_AP1R3\_EL2 are implemented only in implementations that support 7 bits of preemption. Unimplemented registers are **UNDEFINED**.



**Note**

The number of bits of preemption is indicated by AArch64-ICH\_VTR\_EL2.PREbits

Writing to these registers with any value other than the last read value of the register (or 0x00000000 for a newly set up virtual machine) can result in **UNPREDICTABLE** behavior of the virtual interrupt prioritization system allowing either:

Writing to the active priority registers in any order other than the following order will result in **UNPREDICTABLE** behavior:

MRS <Xt>, ICH\_AP1R<m>\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1001	'0':m[1:0]

MSR ICH\_AP1R<m>\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1001	'0':m[1:0]

Accessibility

ICH\_AP1R1\_EL2 is implemented only in implementations that support 6 or more bits of preemption. ICH\_AP1R2\_EL2 and ICH\_AP1R3\_EL2 are implemented only in implementations that support 7 bits of preemption. Unimplemented registers are UNDEFINED.



The number of bits of preemption is indicated by AArch64-ICH\_VTR\_EL2.PREbits

Writing to these registers with any value other than the last read value of the register (or 0x00000000 for a newly set up virtual machine) can result in UNPREDICTABLE behavior of the virtual interrupt prioritization system allowing either:

Writing to the active priority registers in any order other than the following order will result in UNPREDICTABLE behavior:  
MRS <Xt>, ICH\_AP1R<m>\_EL2

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_AP1R_EL2[m];
```

MSR ICH\_AP1R<m>\_EL2, <Xt>

```
integer m = UInt(op2<1:0>);

if m == 1 then
    UNDEFINED;
elseif m == 2 || m == 3 then
    UNDEFINED;
elseif PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ICH_AP1R_EL2[m] = X[t, 64];
```

A.2.6.39 ICC\_SRE\_EL2, Interrupt Controller System Register Enable Register (EL2)

Controls whether the System register interface or the memory-mapped interface to the GIC CPU interface is used for EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-362: AARCH64\_ICC\_SRE\_EL2 bit assignments

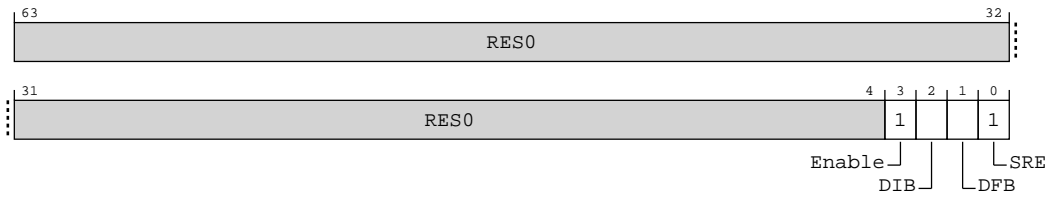


Table A-918: ICC\_SRE\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3]	Enable	Enable. Enables lower Exception level access to AArch64-ICC_SRE_EL1.  0b1  EL1 accesses to AArch64-ICC_SRE_EL1 do not trap to EL2.	0b1



Bits	Name	Description	Reset
[2]	DIB	Disable IRQ bypass.  <b>0b0</b> IRQ bypass enabled.  <b>0b1</b> IRQ bypass disabled.	0b0
[1]	DFB	Disable FIQ bypass.  <b>0b0</b> FIQ bypass enabled.  <b>0b1</b> FIQ bypass disabled.	0b0
[0]	SRE	System Register Enable.  <b>0b1</b> The System register interface to the ICH_* registers and the EL1 and EL2 ICC_* registers is enabled for EL2.	0b1

## Access

Execution with AArch64-ICC\_SRE\_EL2.SRE set to 0 might make some System registers **UNKNOWN**.

MRS <Xt>, ICC\_SRE\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1001	0b101

MSR ICC\_SRE\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1001	0b101

## Accessibility

Execution with AArch64-ICC\_SRE\_EL2.SRE set to 0 might make some System registers UNKNOWN.

MRS <Xt>, ICC\_SRE\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ICC_SRE_EL2;
```

MSR ICC\_SRE\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    ICC_SRE_EL2 = X[t, 64];
```

A.2.6.40 ICH\_HCR\_EL2, Interrupt Controller Hyp Control Register

Controls the environment for VMs.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0xxx	xxxx	xxxx	x0x0	00xx	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-363: AARCH64\_ICH\_HCR\_EL2 bit assignments

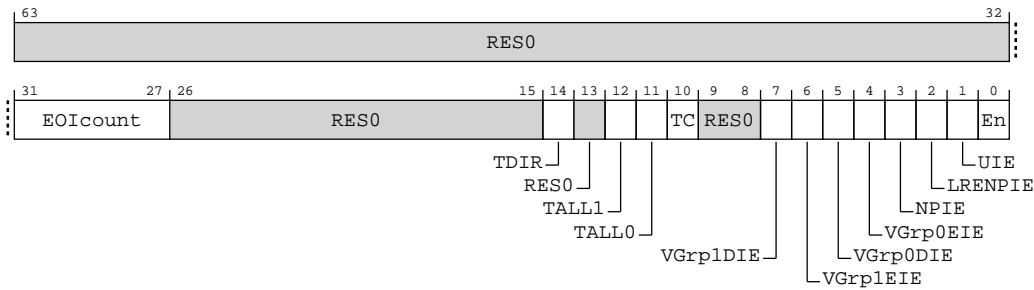


Table A-921: ICH\_HCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:27]	EOLcount	<p>This field is incremented whenever a successful write to a virtual EOIR or DIR register would have resulted in a virtual interrupt deactivation. That is either:</p> <ul style="list-style-type: none"> <li>A virtual write to EOIR with a valid interrupt identifier that is not in the LPI range (that is &lt; 8192) when EOI mode is zero and no List Register was found.</li> <li>A virtual write to DIR with a valid interrupt identifier that is not in the LPI range (that is &lt; 8192) when EOI mode is one and no List Register was found.</li> </ul> <p>This allows software to manage more active interrupts than there are implemented List Registers.</p> <p>It is <b>CONSTRAINED UNPREDICTABLE</b> whether a virtual write to EOIR that does not clear a bit in the Active Priorities registers (AArch64-ICH_AP0R&lt;n&gt;_EL2/AArch64-ICH_AP1R&lt;n&gt;_EL2) increments EOLcount. The implemented behavior is to leave EOLcount unchanged.</p>	0b00000
[26:15]	RES0	Reserved	RES0
[14]	TDIR	<p>Trap EL1 writes to AArch64-ICC_DIR_EL1 and AArch64-ICV_DIR_EL1.</p> <p><b>0b0</b></p> <p>EL1 writes of AArch64-ICC_DIR_EL1 and AArch64-ICV_DIR_EL1 are not trapped to EL2, unless trapped by other mechanisms.</p> <p><b>0b1</b></p> <p>EL1 writes of AArch64-ICV_DIR_EL1 and AArch64-ICC_DIR_EL1 are trapped to EL2.</p>	0b0
[13]	RES0	Reserved	RES0
[12]	TALL1	<p>Trap all EL1 accesses to ICC_* and ICV_* System registers for Group 1 interrupts to EL2.</p> <p><b>0b0</b></p> <p>EL1 accesses to ICC_* and ICV_* registers for Group 1 interrupts proceed as normal.</p> <p><b>0b1</b></p> <p>EL1 accesses to ICC_* and ICV_* registers for Group 1 interrupts trap to EL2.</p>	0b0
[11]	TALLO	<p>Trap all EL1 accesses to ICC_* and ICV_* System registers for Group 0 interrupts to EL2.</p> <p><b>0b0</b></p> <p>EL1 accesses to ICC_* and ICV_* registers for Group 0 interrupts proceed as normal.</p> <p><b>0b1</b></p> <p>EL1 accesses to ICC_* and ICV_* registers for Group 0 interrupts trap to EL2.</p>	0b0
[10]	TC	<p>Trap all EL1 accesses to System registers that are common to Group 0 and Group 1 to EL2.</p> <p><b>0b0</b></p> <p>EL1 accesses to common registers proceed as normal.</p> <p><b>0b1</b></p> <p>EL1 accesses to common registers trap to EL2.</p> <p>This affects accesses to AArch64-ICC_SGI0R_EL1, AArch64-ICC_SGI1R_EL1, AArch64-ICC_ASGI1R_EL1, AArch64-ICC_CTLR_EL1, AArch64-ICC_DIR_EL1, AArch64-ICC_PMR_EL1, AArch64-ICC_RPR_EL1, AArch64-ICV_CTLR_EL1, AArch64-ICV_DIR_EL1, AArch64-ICV_PMR_EL1, and AArch64-ICV_RPR_EL1.</p>	0b0
[9:8]	RES0	Reserved	RES0
[7]	VGrp1DIE	<p>VM Group 1 Disabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 1 interrupts from the virtual CPU interface to the connected vPE is disabled:</p> <p><b>0b0</b></p> <p>Maintenance interrupt disabled.</p> <p><b>0b1</b></p> <p>Maintenance interrupt signaled when AArch64-ICH_VMCR_EL2.VENG1 is 0.</p>	0b0

Bits	Name	Description	Reset
[6]	VGrp1EIE	<p>VM Group 1 Enabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 1 interrupts from the virtual CPU interface to the connected vPE is enabled:</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt signaled when AArch64-ICH_VMCR_EL2.VENG1 is 1.</p>	0b0
[5]	VGrp0DIE	<p>VM Group 0 Disabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 0 interrupts from the virtual CPU interface to the connected vPE is disabled:</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt signaled when AArch64-ICH_VMCR_EL2.VENG0 is 0.</p>	0b0
[4]	VGrp0EIE	<p>VM Group 0 Enabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 0 interrupts from the virtual CPU interface to the connected vPE is enabled:</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt signaled when AArch64-ICH_VMCR_EL2.VENG0 is 1.</p>	0b0
[3]	NPiE	<p>No Pending Interrupt Enable. Enables the signaling of a maintenance interrupt when there are no List registers with the State field set to 0b01 (pending):</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt signaled while the List registers contain no interrupts in the pending state.</p>	0b0
[2]	LRENPiE	<p>List Register Entry Not Present Interrupt Enable. Enables the signaling of a maintenance interrupt while the virtual CPU interface does not have a corresponding valid List register entry for an EOI request:</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt is asserted while the EOICount field is not 0.</p>	0b0
[1]	UIE	<p>Underflow Interrupt Enable. Enables the signaling of a maintenance interrupt when the List registers are empty, or hold only one valid entry:</p> <p><b>0b0</b> Maintenance interrupt disabled.</p> <p><b>0b1</b> Maintenance interrupt is asserted if none, or only one, of the List register entries is marked as a valid interrupt.</p>	0b0

Bits	Name	Description	Reset
[0]	En	Enable. Global enable bit for the virtual CPU interface:  <b>0b0</b> Virtual CPU interface operation disabled.  <b>0b1</b> Virtual CPU interface operation enabled.  When this field is set to 0: <ul style="list-style-type: none"><li>• The virtual CPU interface does not signal any maintenance interrupts.</li><li>• The virtual CPU interface does not signal any virtual interrupts.</li><li>• A read of AArch64-ICV_IAR0_EL1, AArch64-ICV_IAR1_EL1, ext-GICV_IAR or ext-GICV_AIAR returns a spurious interrupt ID.</li></ul>	0b0

Access

MRS <Xt>, ICH\_HCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b000

MSR ICH\_HCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b000

Accessibility

MRS <Xt>, ICH\_HCR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_HCR_EL2;
```

MSR ICH\_HCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ICH_HCR_EL2 = X[t, 64];
```

A.2.6.41 ICH\_VTR\_EL2, Interrupt Controller VGIC Type Register

Reports supported GIC virtualization features.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001	0000	0011	10xx	xxxx	xxxx	xxx0	0011
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-364: AARCH64\_ICH\_VTR\_EL2 bit assignments

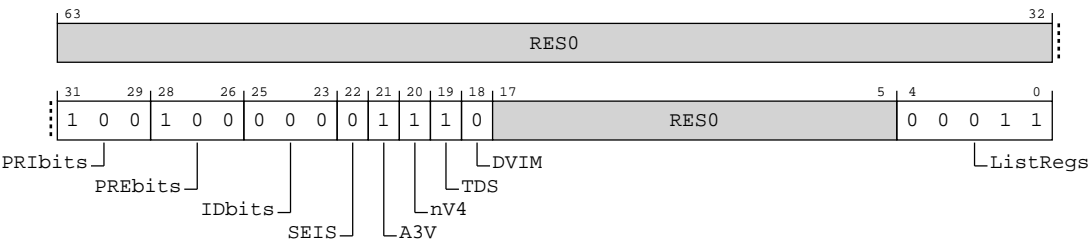


Table A-924: ICH\_VTR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:29]	PRIbits	<p>Priority bits. The number of virtual priority bits implemented, minus one.</p> <p>An implementation must implement at least 32 levels of virtual priority (5 priority bits).</p> <p>This field is an alias of AArch64-ICV_CTLR_EL1.PRIbits.</p> <p><b>0b100</b></p> <p>5 virtual priority bits are implemented.</p>	0b100
[28:26]	PREbits	<p>The number of virtual preemption bits implemented, minus one. This field determines the minimum value of AArch64-ICH_VMCR_EL2.VBPR0.</p> <p><b>0b100</b></p> <p>5 virtual preemption bits are implemented.</p>	0b100
[25:23]	IDbits	<p>The number of virtual interrupt identifier bits supported:</p> <p><b>0b000</b></p> <p>16 bits.</p> <p>All other values are reserved.</p> <p>This field is an alias of AArch64-ICV_CTLR_EL1.IDbits.</p>	0b000
[22]	SEIS	<p>SEI Support. Indicates whether the virtual CPU interface supports generation of SEIs:</p> <p><b>0b0</b></p> <p>The virtual CPU interface logic does not support generation of SEIs.</p> <p>This bit is an alias of AArch64-ICV_CTLR_EL1.SEIS.</p>	0b0
[21]	A3V	<p>Affinity 3 Valid. Possible values are:</p> <p><b>0b1</b></p> <p>The virtual CPU interface logic supports nonzero values of Affinity 3 in SGI generation System registers.</p> <p>This bit is an alias of AArch64-ICV_CTLR_EL1.A3V.</p>	0b1
[20]	nV4	<p>Direct injection of virtual interrupts not supported. Possible values are:</p> <p><b>0b1</b></p> <p>The CPU interface logic does not support direct injection of virtual interrupts.</p>	0b1
[19]	TDS	<p>Separate trapping of EL1 writes to AArch64-ICV_DIR_EL1 supported.</p> <p><b>0b1</b></p> <p>Implementation supports AArch64-ICH_HCR_EL2.TDIR.</p>	0b1
[18]	DVIM	<p>Masking of directly-injected virtual interrupts.</p> <p><b>0b0</b></p> <p>Masking of Directly-injected Virtual Interrupts not supported.</p>	0b0
[17:5]	RES0	Reserved	RES0
[4:0]	ListRegs	<p>The number of implemented List registers, minus one.</p> <p><b>0b00011</b></p> <p>4 List registers implemented.</p>	0b00011

## Access

MRS <Xt>, ICH\_VTR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b001

Accessibility

MRS <Xt>, ICH\_VTR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ICH_VTR_EL2;
```

A.2.6.42 ICH\_MISR\_EL2, Interrupt Controller Maintenance Interrupt State Register

Indicates which maintenance interrupts are asserted.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



## Bit descriptions

Figure A-365: AARCH64\_ICH\_MISR\_EL2 bit assignments

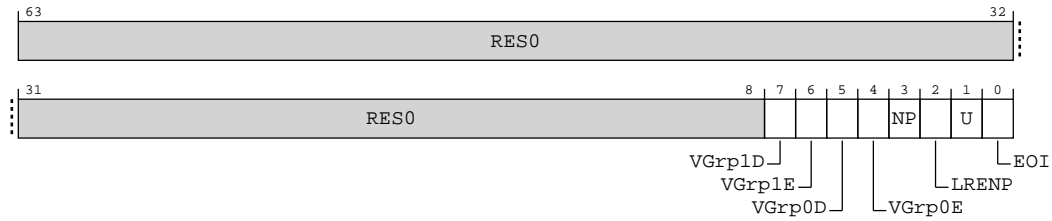


Table A-926: ICH\_MISR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7]	VGrp1D	<p>vPE Group 1 Disabled.</p> <p><b>0b0</b></p> <p>vPE Group 1 Disabled maintenance interrupt not asserted.</p> <p><b>0b1</b></p> <p>vPE Group 1 Disabled maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.VGrp1DIE==1 and AArch64-ICH_VMCR_EL2.VENG1==is 0.</p>	0b0
[6]	VGrp1E	<p>vPE Group 1 Enabled.</p> <p><b>0b0</b></p> <p>vPE Group 1 Enabled maintenance interrupt not asserted.</p> <p><b>0b1</b></p> <p>vPE Group 1 Enabled maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.VGrp1EIE==1 and AArch64-ICH_VMCR_EL2.VENG1==is 1.</p>	0b0
[5]	VGrp0D	<p>vPE Group 0 Disabled.</p> <p><b>0b0</b></p> <p>vPE Group 0 Disabled maintenance interrupt not asserted.</p> <p><b>0b1</b></p> <p>vPE Group 0 Disabled maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.VGrp0DIE==1 and AArch64-ICH_VMCR_EL2.VENG0==0.</p>	0b0
[4]	VGrp0E	<p>vPE Group 0 Enabled.</p> <p><b>0b0</b></p> <p>vPE Group 0 Enabled maintenance interrupt not asserted.</p> <p><b>0b1</b></p> <p>vPE Group 0 Enabled maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.VGrp0EIE==1 and AArch64-ICH_VMCR_EL2.VENG0==1.</p>	0b0

Bits	Name	Description	Reset
[3]	NP	<p>No Pending.</p> <p><b>0b0</b> No Pending maintenance interrupt not asserted.</p> <p><b>0b1</b> No Pending maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.NPIE==1 and no List register is in pending state.</p>	0b0
[2]	LRENP	<p>List Register Entry Not Present.</p> <p><b>0b0</b> List Register Entry Not Present maintenance interrupt not asserted.</p> <p><b>0b1</b> List Register Entry Not Present maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.LRENPIE==1 and AArch64-ICH_HCR_EL2.EOIcount is nonzero.</p>	0b0
[1]	U	<p>Underflow.</p> <p><b>0b0</b> Underflow maintenance interrupt not asserted.</p> <p><b>0b1</b> Underflow maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when AArch64-ICH_HCR_EL2.UIE==1 and zero or one of the List register entries are marked as a valid interrupt, that is, if the corresponding AArch64-ICH_LR&lt;n&gt;_EL2.State bits do not equal 0x0.</p>	0b0
[0]	EOI	<p>End Of Interrupt.</p> <p><b>0b0</b> End Of Interrupt maintenance interrupt not asserted.</p> <p><b>0b1</b> End Of Interrupt maintenance interrupt asserted.</p> <p>This maintenance interrupt is asserted when at least one bit in AArch64-ICH_EISR_EL2 is 1.</p>	0b0

The U and NP bits do not include the status of any pending/active 'VSet (IRI)' in ARM® Generic Interrupt Controller Architecture Specification, GIC architecture version 3.0 and version 4.0 (ARM IHI 0069) packets because these bits control generation of interrupts that allow software management of the contents of the List Registers (which are not affected by 'VSet (IRI)' packets).

## Access

MRS <Xt>, ICH\_MISR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b010

Accessibility

MRS <Xt>, ICH\_MISR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ICH_MISR_EL2;
```

A.2.6.43 ICH\_EISR\_EL2, Interrupt Controller End of Interrupt Status Register

Indicates which List registers have outstanding EOI maintenance interrupts.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
0															



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-366: AARCH64\_ICH\_EISR\_EL2 bit assignments

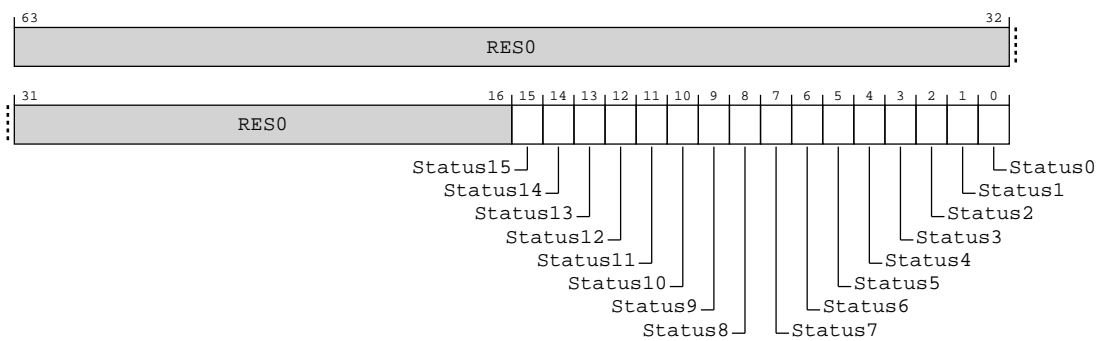


Table A-928: ICH\_EISR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0
[15:0]	Status<n>	<p>EOI maintenance interrupt status bit for List register &lt;n&gt;:</p> <p><b>0b0</b></p> <p>List register &lt;n&gt;, AArch64-ICH_LR&lt;n&gt;_EL2, does not have an EOI maintenance interrupt.</p> <p><b>0b1</b></p> <p>List register &lt;n&gt;, AArch64-ICH_LR&lt;n&gt;_EL2, has an EOI maintenance interrupt that has not been handled.</p> <p>For any AArch64-ICH_LR&lt;n&gt;_EL2, the corresponding status bit is set to 1 if all of the following are true:</p> <ul style="list-style-type: none"><li>AArch64-ICH_LR&lt;n&gt;_EL2.State is 0b00.</li><li>AArch64-ICH_LR&lt;n&gt;_EL2.HW is 0.</li><li>AArch64-ICH_LR&lt;n&gt;_EL2.EOI (bit [41]) is 1, indicating that when the interrupt corresponding to that List register is deactivated, a maintenance interrupt is asserted.</li></ul> <p>Otherwise the status bit takes the value 0.</p>	16{x}

Access

MRS <Xt>, ICH\_EISR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b011

Accessibility

MRS <Xt>, ICH\_EISR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_EISR_EL2;
```

A.2.6.44 ICH\_ELRSR\_EL2, Interrupt Controller Empty List Register Status Register

These registers can be used to locate a usable List register when the hypervisor is delivering an interrupt to a VM.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-367: AARCH64\_ICH\_ELRSR\_EL2 bit assignments

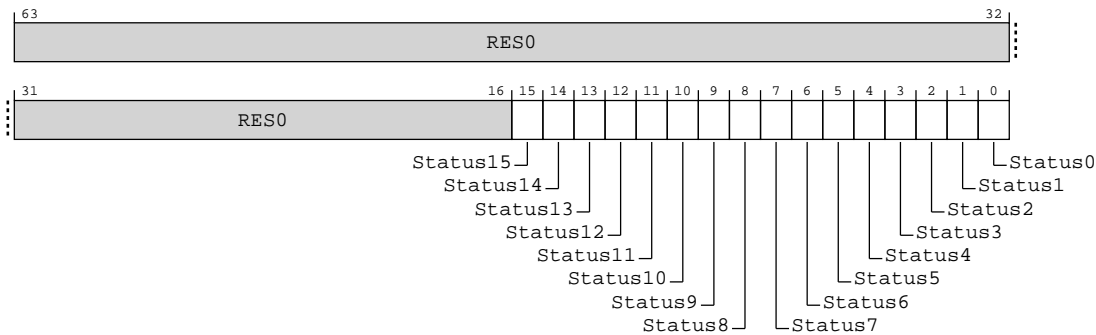


Table A-930: ICH\_ELRSR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[15:0]	Status<n>	<div>Status bit for List register &lt;n&gt;, AArch64-ICH_LR&lt;n&gt;_EL2:</div> <div><div>0b0</div><div>List register AArch64-ICH_LR&lt;n&gt;_EL2, if implemented, contains a valid interrupt. Using this List register can result in overwriting a valid interrupt.</div></div> <div><div>0b1</div><div>List register AArch64-ICH_LR&lt;n&gt;_EL2 does not contain a valid interrupt. The List register is empty and can be used without overwriting a valid interrupt or losing an EOI maintenance interrupt.</div></div> <div>For any List register &lt;n&gt;, the corresponding status bit is set to 1 if AArch64-ICH_LR&lt;n&gt;_EL2.State is 0b00 and either AArch64-ICH_LR&lt;n&gt;_EL2.HW is 1 or AArch64-ICH_LR&lt;n&gt;_EL2.EOI (bit [41]) is 0.</div> <div>Otherwise the status bit takes the value 0.</div>	16 {x}

Access

MRS <Xt>, ICH\_ELRSR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b101

Accessibility

MRS <Xt>, ICH\_ELRSR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_ELRSR_EL2;
```

A.2.6.45 ICH\_VMCR\_EL2, Interrupt Controller Virtual Machine Control Register

Enables the hypervisor to save and restore the virtual machine view of the GIC state.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

GIC system registers

Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-368: AARCH64\_ICH\_VMCR\_EL2 bit assignments

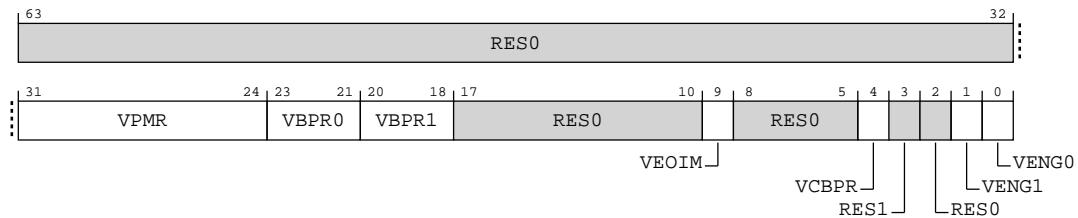


Table A-932: ICH\_VMCR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:24]	VPMR	Virtual Priority Mask. The priority mask level for the virtual CPU interface. If the priority of a pending virtual interrupt is higher than the value indicated by this field, the interface signals the virtual interrupt to the PE.  This field is an alias of AArch64-ICV_PMR_EL1.Priority.	8{x}
[23:21]	VBPR0	Virtual Binary Point Register, Group 0. Defines the point at which the priority value fields split into two parts, the group priority field and the subpriority field. The group priority field determines Group 0 interrupt preemption, and also determines Group 1 interrupt preemption if ICH_VMCR_EL2.VCBPR == 1.  This field is an alias of AArch64-ICV_BPR0_EL1.BinaryPoint.  The minimum value of this field is determined by AArch64-ICH_VTR_EL2.PREbits. An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value.	xxx
[20:18]	VBPR1	Virtual Binary Point Register, Group 1. Defines the point at which the priority value fields split into two parts, the group priority field and the subpriority field. The group priority field determines Group 1 interrupt preemption if AArch64-ICH_VMCR_EL2.VCBPR == 0.  This field is an alias of AArch64-ICV_BPR1_EL1.BinaryPoint.  This field is always accessible to EL2 accesses, regardless of the setting of the ICH_VMCR_EL2.VCBPR field.  For Secure writes, the minimum value of this field is the minimum value of ICH_VMCR_EL2.VBPR0.  An attempt to program the binary point field to a value less than the minimum value sets the field to the minimum value.	xxx

Bits	Name	Description	Reset
[17:10]	<b>RES0</b>	Reserved	<b>RES0</b>
[9]	VEOIM	<p>Virtual EOI mode. Controls whether a write to an End of Interrupt register also deactivates the virtual interrupt:</p> <p><b>0b0</b></p> <p>AArch64-ICV_EOIR0_EL1 and AArch64-ICV_EOIR1_EL1 provide both priority drop and interrupt deactivation functionality. Accesses to AArch64-ICV_DIR_EL1 are <b>UNPREDICTABLE</b>.</p> <p><b>0b1</b></p> <p>AArch64-ICV_EOIR0_EL1 and AArch64-ICV_EOIR1_EL1 provide priority drop functionality only. AArch64-ICV_DIR_EL1 provides interrupt deactivation functionality.</p> <p>This bit is an alias of AArch64-ICV_CTLR_EL1.EOImode.</p>	x
[8:5]	<b>RES0</b>	Reserved	<b>RES0</b>
[4]	VCBPR	<p>Virtual Common Binary Point Register. Possible values of this bit are:</p> <p><b>0b0</b></p> <p>AArch64-ICV_BPR1_EL1 determines the preemption group for virtual Group 1 interrupts.</p> <p><b>0b1</b></p> <p>Reads of AArch64-ICV_BPR1_EL1 return AArch64-ICV_BPR0_EL1 plus one, saturated to 0b111. Writes to AArch64-ICV_BPR1_EL1 are ignored.</p> <p>This field is an alias of AArch64-ICV_CTLR_EL1.CBPR.</p>	x
[3]	<b>RES1</b>	Reserved	<b>RES1</b>
[2]	<b>RES0</b>	Reserved	<b>RES0</b>
[1]	VENG1	<p>Virtual Group 1 interrupt enable. Possible values of this bit are:</p> <p><b>0b0</b></p> <p>Virtual Group 1 interrupts are disabled.</p> <p><b>0b1</b></p> <p>Virtual Group 1 interrupts are enabled.</p> <p>This bit is an alias of AArch64-ICV_IGRPEN1_EL1.Enable.</p>	x
[0]	VENG0	<p>Virtual Group 0 interrupt enable. Possible values of this bit are:</p> <p><b>0b0</b></p> <p>Virtual Group 0 interrupts are disabled.</p> <p><b>0b1</b></p> <p>Virtual Group 0 interrupts are enabled.</p> <p>This bit is an alias of AArch64-ICV_IGRPEN0_EL1.Enable.</p>	x

## Access

When EL2 is using System register access, EL1 using either System register or memory-mapped access must be supported.

MRS <Xt>, ICH\_VMCR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b111



MSR ICH\_VMCR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b111

Accessibility

When EL2 is using System register access, EL1 using either System register or memory-mapped access must be supported.

MRS <Xt>, ICH\_VMCR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ICH_VMCR_EL2;
```

MSR ICH\_VMCR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ICH_VMCR_EL2 = X[t, 64];
```

A.2.7 AArch64 RAS register description

This section includes the register descriptions for all *Reliability, Availability, and Serviceability* (RAS) registers in the Cortex®-R82AE processor.

A.2.7.1 ERRIDR\_EL1, Error Record ID Register

Defines the highest numbered index of the error records that can be accessed through the Error Record System registers.

Configurations

This register is available in all configurations.

Attributes

Width

64

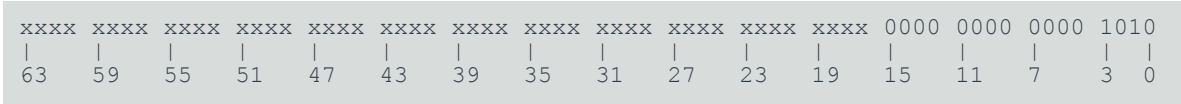
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-369: AARCH64\_ERRIDR\_EL1 bit assignments

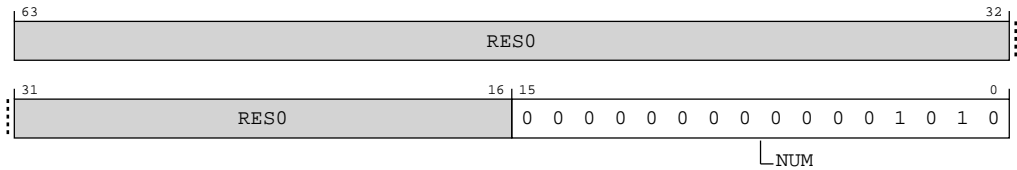


Table A-935: ERRIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0
[15:0]	NUM	Highest numbered index of the records that can be accessed through the Error Record System registers plus one.  0b00000000000001010  10 error records implemented.	0x000A

Access

MRS <Xt>, ERRIDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0011	0b000

Accessibility

MRS <Xt>, ERRIDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERRIDR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = ERRIDR_EL1;
```

A.2.7.2 ERRSELR\_EL1, Error Record Select Register

Selects an error record to be accessed through the Error Record System registers.

Configurations

If AArch64-ERRIDR\_EL1 indicates that zero error records are implemented, then it is IMPLEMENTATION DEFINED whether ERRSELR\_EL1 is UNDEFINED or RES0.

Attributes

Width

64

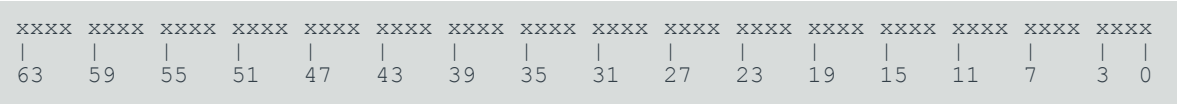
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-370: AARCH64\_ERRSELR\_EL1 bit assignments

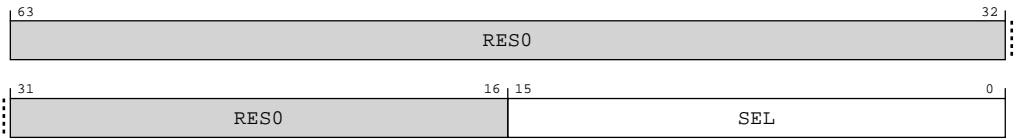


Table A-937: ERRSELR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[15:0]	SEL	<p>Selects the error record accessed through the ERX registers.</p> <p><b>0b0000000000000000</b> Select record 0, containing non-ECC memory errors from L2 cache and LCU.</p> <p><b>0b0000000000000001</b> Select record 1, containing memory errors from L1 I-cache, L1 D-cache, ITCM, DTCM and MMS.</p> <p><b>0b0000000000000010</b> Select record 2, containing memory errors from L1 I-cache, L1 D-cache, ITCM, DTCM and MMS.</p> <p><b>0b0000000000000011</b> Select record 3, containing memory errors from L1 I-cache, L1 D-cache, ITCM, DTCM and MMS.</p> <p><b>0b0000000000000100</b> Select record 4, containing memory errors from L2 cache and LCU.</p> <p><b>0b0000000000000101</b> Select record 5, containing memory errors from L2 cache and LCU.</p> <p><b>0b0000000000000110</b> Select record 6, containing memory errors from L2 cache and LCU.</p> <p><b>0b0000000000000111</b> Select record 7, containing errors detected from the cores by the safety mechanisms.</p> <p><b>0b0000000000001000</b> Select record 8, containing errors detected from the cluster by the safety mechanisms.</p> <p><b>0b0000000000001001</b> Select record 9, containing errors detected from the cluster by the safety mechanisms.</p> <p>For example, if ERRSELR_EL1.SEL is 0x0004, then direct reads and writes of AArch64-ERXSTATUS_EL1 access ERR4STATUS.</p> <p>If ERRSELR_EL1.SEL is greater than or equal to AArch64-ERRIDR_EL1.NUM, then all of the following apply:</p> <ul style="list-style-type: none"> <li>• The value read back from ERRSELR_EL1.SEL is <b>UNKNOWN</b>.</li> <li>• One of the following occurs: <ul style="list-style-type: none"> <li>◦ An <b>UNKNOWN</b> error record is selected.</li> <li>◦ The ERX*_EL1 registers are RAZ/WI.</li> </ul> </li> </ul>	16 {x}

## Access

MRS <Xt>, ERRSELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0011	0b001

MSR ERRSELR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0011	0b001

Accessibility

MRS <Xt>, ERRSELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERRSELR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ERRSELR_EL1;
```

MSR ERRSELR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERRSELR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ERRSELR_EL1 = X[t, 64];
```

A.2.7.3 ERXFR\_EL1, Selected Error Record Feature Register

Accesses ext-ERR<n>FR for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-371: AARCH64\_ERXFR\_EL1 bit assignments

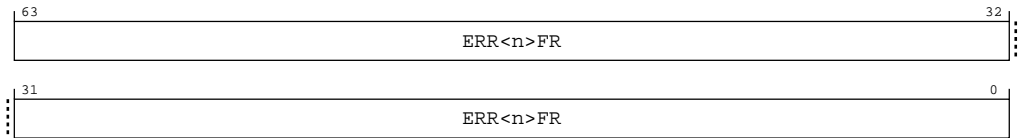


Table A-940: ERXFR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXFR_EL1 accesses ext-ERR<n>FR, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXFR\_EL1 is RAZ.

MRS <Xt>, ERXFR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b000

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXFR\_EL1 is RAZ.

MRS <Xt>, ERXFR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXFR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXFR_EL1;
```

A.2.7.4 ERXCTLR\_EL1, Selected Error Record Control Register

Accesses ext-ERR<n>CTLR for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

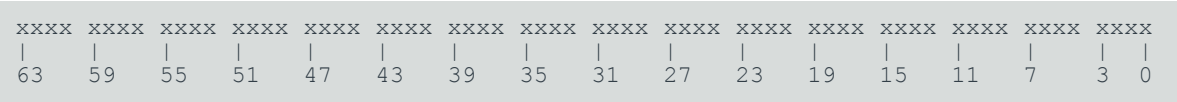
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-372: AARCH64\_ERXCTLR\_EL1 bit assignments

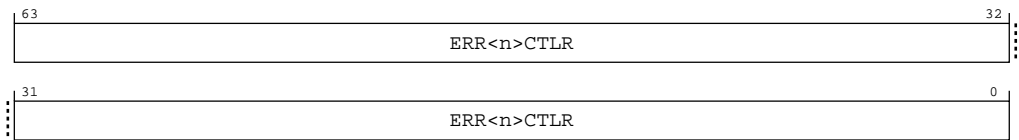


Table A-942: ERXCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXCTLR_EL1 accesses ext-ERR<n>CTLR, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXCTLR\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>CTLR is not present, meaning reads and writes of ERXCTLR\_EL1 are **RES0**.

MRS <Xt>, ERXCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b001

MSR ERXCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b001

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An UNKNOWN error record is selected.
- ERXCTLR\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>CTLR is not present, meaning reads and writes of ERXCTLR\_EL1 are RES0.

MRS <Xt>, ERXCTLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXCTLR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ERXCTLR_EL1;
```

MSR ERXCTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXCTLR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ERXCTLR_EL1 = X[t, 64];
```



A.2.7.5 ERXSTATUS\_EL1, Selected Error Record Primary Status Register

Accesses ext-ERR<n>STATUS for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-373: AARCH64\_ERXSTATUS\_EL1 bit assignments

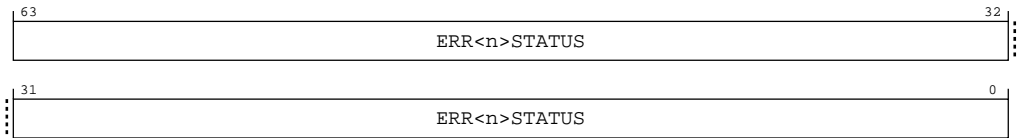


Table A-945: ERXSTATUS\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXSTATUS_EL1 accesses ext-ERR<n>STATUS, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 { x }

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXSTATUS\_EL1 is RAZ/WI.

ext-ERR<n>STATUS describes additional constraints that also apply when ext-ERR<n>STATUS is accessed through ERXSTATUS\_EL1.

MRS <Xt>, ERXSTATUS\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b010

MSR ERXSTATUS\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b010

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An UNKNOWN error record is selected.
- ERXSTATUS\_EL1 is RAZ/WI.

ext-ERR<n>STATUS describes additional constraints that also apply when ext-ERR<n>STATUS is accessed through ERXSTATUS\_EL1.

MRS <Xt>, ERXSTATUS\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXSTATUS_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXSTATUS_EL1;
```

MSR ERXSTATUS\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXSTATUS_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXSTATUS_EL1 = X[t, 64];
```

A.2.7.6 ERXADDR\_EL1, Selected Error Record Address Register

Accesses ext-ERR<n>ADDR for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

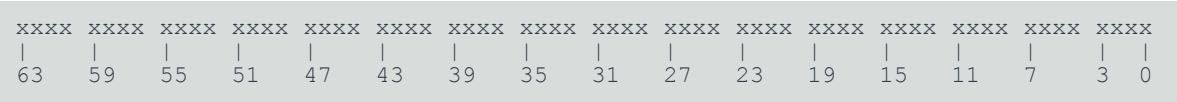
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-374: AARCH64\_ERXADDR\_EL1 bit assignments

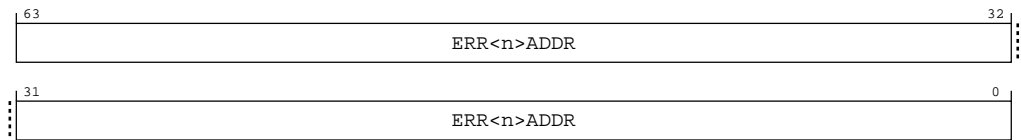


Table A-948: ERXADDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXADDR_EL1 accesses ext-ERR<n>ADDR, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 { x }

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXADDR\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXADDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b011

MSR ERXADDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b011

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXADDR\_EL1 is RAZ/WI.  
MRS <Xt>, ERXADDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXADDR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXADDR_EL1;
```

MSR ERXADDR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXADDR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXADDR_EL1 = X[t, 64];
```

A.2.7.7 ERXPFGF\_EL1, Selected Pseudo-fault Generation Feature Register

Accesses ext-ERR<n>PFGF for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

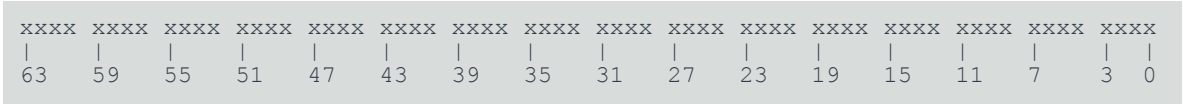
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-375: AArch64\_ERXPFGF\_EL1 bit assignments

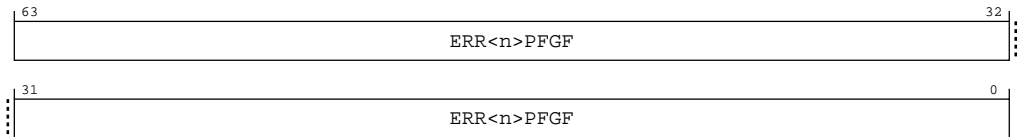


Table A-951: ERXPFGF\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXPFGF_EL1 accesses ext-ERR<n>PFGF, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 { x }

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXPFGF\_EL1 is RAZ.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads of ERXPFGF\_EL1 are NOPs.



A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGF is not present, meaning reads of ERXPFGF\_EL1 are **RES0**.

ext-ERR<n>PFGF describes additional constraints that also apply when ext-ERR<n>PFGF is accessed through ERXPFGF\_EL1.

MRS <Xt>, ERXPFGF\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b100

### Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An UNKNOWN error record is selected.
- ERXPFGF\_EL1 is RAZ.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads of ERXPFGF\_EL1 are NOPs.



A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGF is not present, meaning reads of ERXPFGF\_EL1 are RES0.

ext-ERR<n>PFGF describes additional constraints that also apply when ext-ERR<n>PFGF is accessed through ERXPFGF\_EL1.

MRS <Xt>, ERXPFGF\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.FIEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXPFGF_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXPFGF_EL1;

```

### A.2.7.8 ERXPFGCTL\_EL1, Selected Pseudo-fault Generation Control Register

Accesses ext-ERR<n>PFGCTL for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-376: AARCH64\_ERXPGCTL\_EL1 bit assignments

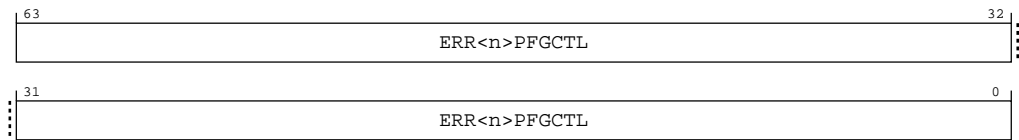


Table A-953: ERXPGCTL\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXPGCTL_EL1 accesses ext-ERR<n>PFGCTL, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXPGCTL\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads and writes of ERXPGCTL\_EL1 are NOPs.



A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGCTL is not present, meaning reads and writes of ERXPFGCTL\_EL1 are **RES0**.

ext-ERR<n>PFGCTL describes additional constraints that also apply when ext-ERR<n>PFGCTL is accessed through ERXPFGCTL\_EL1.

MRS <Xt>, ERXPFGCTL\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b101

MSR ERXPFGCTL\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b101

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An UNKNOWN error record is selected.
- ERXPFGCTL\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads and writes of ERXPFGCTL\_EL1 are NOPs.



Note

A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGCTL is not present, meaning reads and writes of ERXPFGCTL\_EL1 are RES0.

ext-ERR<n>PFGCTL describes additional constraints that also apply when ext-ERR<n>PFGCTL is accessed through ERXPFGCTL\_EL1.

MRS <Xt>, ERXPFGCTL\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.FIEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXPFGCTL_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = ERXPFGCTL_EL1;
```



MSR ERXPGCTL\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.FIEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXPGCTL_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ERXPGCTL_EL1 = X[t, 64];
```

A.2.7.9 ERXPGCDN\_EL1, Selected Pseudo-fault Generation Countdown Register

Accesses ext-ERR<n>PFGCDN for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

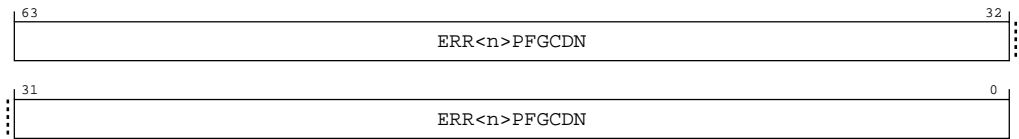


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-377: AARCH64\_ERXPGCDN\_EL1 bit assignments



**Table A-956: ERXPFGCDN\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	None	ERXPFGCDN_EL1 accesses ext-ERR<n>PFGCDN, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

### Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXPFGCDN\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads and writes of ERXPFGCDN\_EL1 are NOPs.

**Note**

A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGCDN is not present, meaning reads and writes of ERXPFGCDN\_EL1 are **RESO**.

ext-ERR<n>PFGCDN describes additional constraints that also apply when ext-ERR<n>PFGCDN is accessed through ERXPFGCDN\_EL1.

MRS <Xt>, ERXPFGCDN\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b110

MSR ERXPFGCDN\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0100	0b110

### Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXPFGCDN\_EL1 is RAZ/WI.

If AArch64-ERRSELR\_EL1.SEL selects an error record owned by a node that does not implement the Common Fault Injection Model Extension, then direct reads and writes of ERXPFGCDN\_EL1 are NOPs.



A node does not implement the Common Fault Injection Model Extension if ERR<q>FR.INJ reads as 0b00. <q> is the index of the first error record owned by the same node as error record <n>, where <n> is the value in AArch64-ERRSELR\_EL1.SEL. If the node owns a single record, then q = n.

If AArch64-ERRSELR\_EL1.SEL is not the index of the first error record owned by a node, then ext-ERR<n>PFGCDN is not present, meaning reads and writes of ERXPFGCDN\_EL1 are RES0.

ext-ERR<n>PFGCDN describes additional constraints that also apply when ext-ERR<n>PFGCDN is accessed through ERXPFGCDN\_EL1.

MRS <Xt>, ERXPFGCDN\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.FIEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXPFGCDN_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXPFGCDN_EL1;
```

MSR ERXPFGCDN\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.FIEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXPFGCDN_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXPFGCDN_EL1 = X[t, 64];
```

### A.2.7.10 ERXMISCO\_EL1, Selected Error Record Miscellaneous Register 0

Accesses ext-ERR<n>MISCO for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

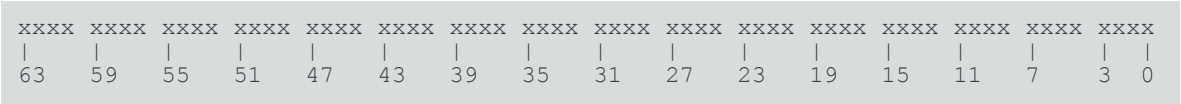
##### Functional group

RAS registers

##### Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-378: AARCH64\_ERXMISC0\_EL1 bit assignments

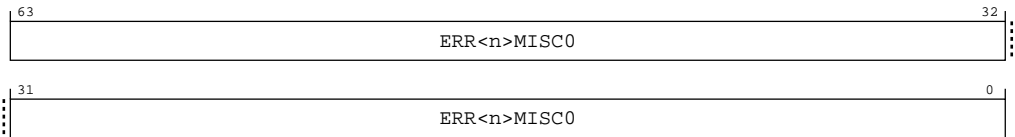


Table A-959: ERXMISC0\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXMISC0_EL1 accesses ext-ERR<n>MISC0, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An **UNKNOWN** error record is selected.
- ERXMISC0\_EL1 is RAZ/WI.

ext-ERR<n>MISC0 describes additional constraints that also apply when ext-ERR<n>MISC0 is accessed through ERXMISC0\_EL1.

MRS <Xt>, ERXMISC0\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b000

MSR ERXMISC0\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b000

## Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then one of the following occurs:

- An UNKNOWN error record is selected.
- ERXMISCO\_EL1 is RAZ/WI.

ext-ERR<n>MISCO describes additional constraints that also apply when ext-ERR<n>MISCO is accessed through ERXMISCO\_EL1.

MRS <Xt>, ERXMISCO\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXMISCO_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXMISCO_EL1;

```

MSR ERXMISCO\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXMISCO_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXMISCO_EL1 = X[t, 64];

```

### A.2.7.11 ERXMISC1\_EL1, Selected Error Record Miscellaneous Register 1

Accesses ext-ERR<n>MISC1 for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

RAS registers

### Access type

See bit descriptions

### Reset value

```

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

```



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-379: AARCH64\_ERXMISC1\_EL1 bit assignments

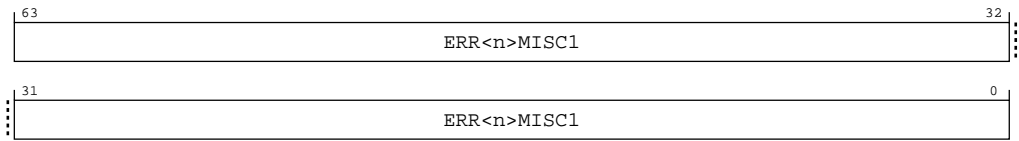


Table A-962: ERXMISC1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXMISC1_EL1 accesses ext-ERR<n>MISC1, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 { x }

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC1\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXMISC1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b001

MSR ERXMISC1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b001

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC1\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXMISC1\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXMISC1_EL1;
    elsif PSTATE.EL == EL2 then
```

```
X[t, 64] = ERXMISC1_EL1;
```

MSR ERXMISC1\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXMISC1_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    ERXMISC1_EL1 = X[t, 64];
```

A.2.7.12 ERXMISC2\_EL1, Selected Error Record Miscellaneous Register 2

Accesses ext-ERR<n>MISC2 for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-380: AARCH64\_ERXMISC2\_EL1 bit assignments

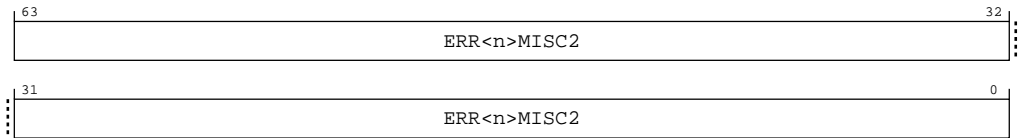


Table A-965: ERXMISC2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXMISC2_EL1 accesses ext-ERR<n>MISC2, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC2\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXMISC2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b010

MSR ERXMISC2\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b010

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC2\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXMISC2\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXMISC2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXMISC2_EL1;
```

MSR ERXMISC2\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```



```
    ERXMISC2_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXMISC2_EL1 = X[t, 64];
```

A.2.7.13 ERXMISC3\_EL1, Selected Error Record Miscellaneous Register 3

Accesses ext-ERR<n>MISC3 for the error record <n> selected by AArch64-ERRSELR\_EL1.SEL.

Configurations

This register is available in all configurations.

Attributes

Width

64

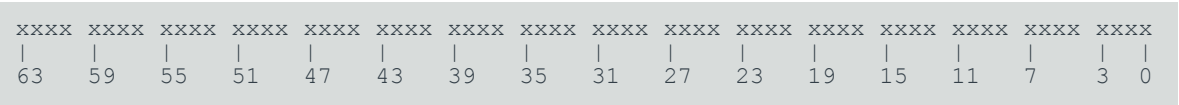
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-381: AARCH64\_ERXMISC3\_EL1 bit assignments

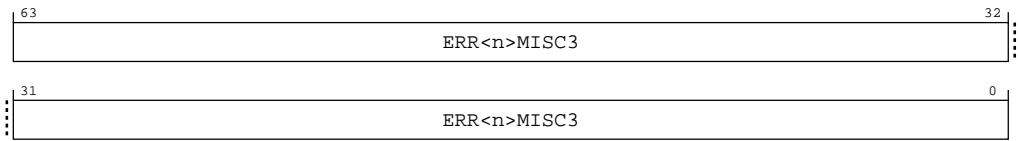


Table A-968: ERXMISC3\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	ERXMISC3_EL1 accesses ext-ERR<n>MISC3, where <n> is the value in AArch64-ERRSELR_EL1.SEL.	64 {x}

Access

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC3\_EL1 is **RAZ/WI**.

MRS <Xt>, ERXMISC3\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b011

MSR ERXMISC3\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0101	0b0101	0b011

Accessibility

If AArch64-ERRSELR\_EL1.SEL is greater than or equal to AArch64-ERRIDR\_EL1.NUM, then ERXMISC3\_EL1 is RAZ/WI.

MRS <Xt>, ERXMISC3\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = ERXMISC3_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ERXMISC3_EL1;
```

MSR ERXMISC3\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TERR == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ERXMISC3_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ERXMISC3_EL1 = X[t, 64];
```

A.2.7.14 DISR\_EL1, Deferred Interrupt Status Register

Records that an SError interrupt has been consumed by an **ESB** instruction.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-382: AARCH64\_DISR\_EL1 bit assignments

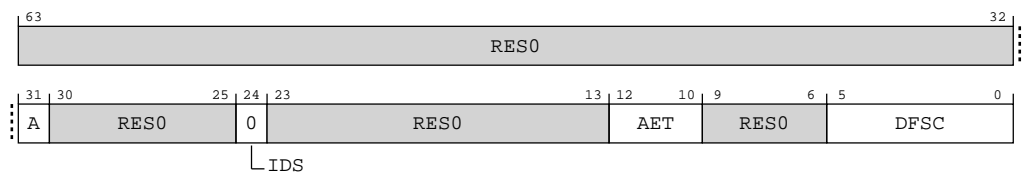


Table A-971: DISR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	A	Set to 1 when an ESB instruction defers an asynchronous SError interrupt.	x
[30:25]	RES0	Reserved	RES0
[24]	IDS	Indicates the deferred SError interrupt type. <b>0b0</b> Deferred error uses architecturally-defined format.	0b0
[23:13]	RES0	Reserved	RES0
[12:10]	AET	Asynchronous Error Type. See the description of ESR_ELx.AET for an SError interrupt.	xxx
[9:6]	RES0	Reserved	RES0
[5:0]	DFSC	Fault Status Code. See the description of ESR_ELx.DFSC for an SError interrupt.	6{x}

Access

An indirect write to DISR\_EL1 made by an `ESB` instruction does not require an explicit synchronization operation for the value that is written to be observed by a direct read of DISR\_EL1 occurring in program order after the `ESB` instruction.

MRS <Xt>, DISR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0001	0b001

MSR DISR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0001	0b001

Accessibility

An indirect write to DISR\_EL1 made by an `ESB` instruction does not require an explicit synchronization operation for the value that is written to be observed by a direct read of DISR\_EL1 occurring in program order after the `ESB` instruction.

MRS <Xt>, DISR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.AMO == '1' then
        X[ $\bar{t}$ , 64] = VDISR_EL2;
    else
        X[t, 64] = DISR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = DISR_EL1;
```

MSR DISR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.AMO == '1' then
        VDISR_EL2 = X[t, 64];
    else
        DISR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    DISR_EL1 = X[t, 64];
```

A.2.7.15 VESR\_EL2, Virtual SError Exception Syndrome Register

Provides the syndrome value reported to software on taking a virtual SError interrupt exception to EL1, or on executing an `ESB` instruction at EL1.

When the virtual SError interrupt injected using AArch64-HCR\_EL2.VSE is taken to EL1 using AArch64, then the syndrome value is reported in AArch64-ESR\_EL1.

When the virtual SError interrupt injected using AArch64-HCR\_EL2.VSE is deferred by an **ESB** instruction, then the syndrome value is written to AArch64-VDISR\_EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

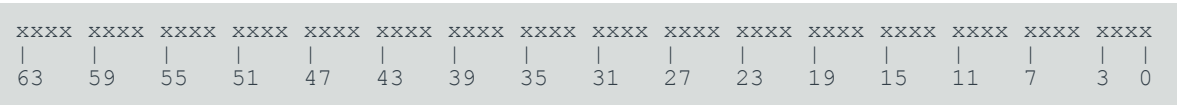
Functional group

RAS registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-383: AARCH64\_VSESR\_EL2 bit assignments

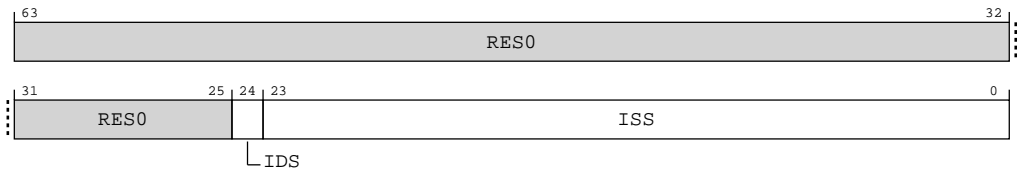


Table A-974: VSESR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:25]	RES0	Reserved	RES0
[24]	IDS	When a virtual SError interrupt is taken to EL1 using AArch64, AArch64-ESR_EL1[24] is set to VSESR_EL2.IDS.  When a virtual SError interrupt is deferred by an <b>ESB</b> instruction, AArch64-VDISR_EL2[24] is set to VSESR_EL2.IDS.	x
[23:0]	ISS	When a virtual SError interrupt is taken to EL1 using AArch64, AArch64-ESR_EL1[23:0] is set to VSESR_EL2.ISS.  When a virtual SError interrupt is deferred by an <b>ESB</b> instruction, AArch64-VDISR_EL2[23:0] is set to VSESR_EL2.ISS.	24 { x }

Access

MRS <Xt>, VSESR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0010	0b011

MSR VSESR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0101	0b0010	0b011

Accessibility

MRS <Xt>, VSESR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VSESR_EL2;
```

MSR VSESR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VSESR_EL2 = X[t, 64];
```

A.2.7.16 VDISR\_EL2, Virtual Deferred Interrupt Status Register

Records that a virtual SError interrupt has been consumed by an **ESB** instruction executed at EL1.

An indirect write to VDISR\_EL2 made by an **ESB** instruction does not require an explicit synchronization operation for the value written to be observed by a direct read of one of the following registers occurring in program order after the **ESB** instruction:

- AArch64-DISR\_EL1.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

RAS registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-384: AARCH64\_VDISR\_EL2 bit assignments

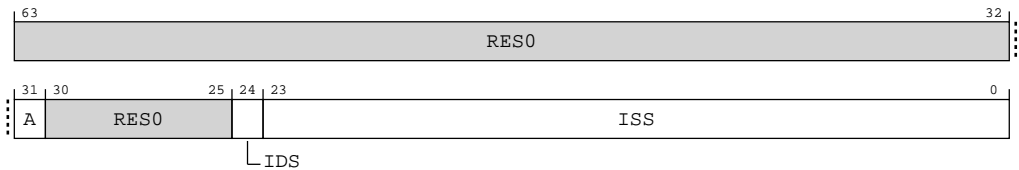


Table A-977: VDISR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	A	Set to 1 when an ESB instruction defers a virtual SError interrupt.	x
[30:25]	RES0	Reserved	RES0
[24]	IDS	The value copied from AArch64-VSESR_EL2.IDS.	x
[23:0]	ISS	The value copied from AArch64-VSESR_EL2.ISS.	24 { x }

Access

An indirect write to VDISR\_EL2 made by an ESB instruction does not require an explicit synchronization operation for the value that is written to be observed by a direct read of one of the following registers occurring in program order after the ESB instruction:

- AArch64-DISR\_EL1.

MRS <Xt>, VDISR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0001	0b001

MSR VDISR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b0001	0b001

MRS &lt;Xt&gt;, DISR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0001	0b001

MSR DISR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1100	0b0001	0b001

### Accessibility

An indirect write to VDISR\_EL2 made by an `ESB` instruction does not require an explicit synchronization operation for the value that is written to be observed by a direct read of one of the following registers occurring in program order after the `ESB` instruction:

- AArch64-DISR\_EL1.

MRS &lt;Xt&gt;, VDISR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = VDISR_EL2;
```

MSR VDISR\_EL2, &lt;Xt&gt;

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    VDISR_EL2 = X[t, 64];
```

MRS &lt;Xt&gt;, DISR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.AMO == '1' then
        X[t, 64] = VDISR_EL2;
    else
        X[t, 64] = DISR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = DISR_EL1;
```

MSR DISR\_EL1, &lt;Xt&gt;

```
if PSTATE.EL == EL0 then
```



```
    UNDEFINED;
    elsif PSTATE.EL == EL1 then
        if HCR_EL2.AMO == '1' then
            VDISR_EL2 = X[t, 64];
        else
            DISR_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        DISR_EL1 = X[t, 64];
```

## A.2.8 AArch64 Trace register description

This section includes the register descriptions for all Trace registers in the Cortex®-R82AE processor.

### A.2.8.1 TRCSEQEVR<n>, Sequencer State Transition Control Register <n> , n = 0 - 2

Moves the sequencer state:

- Backwards, from state n+1 to state n when a programmed resource event occurs.
- Forwards, from state n to state n+1 when a programmed resource event occurs.

#### Configurations

AArch64 register TRCSEQEVR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.19 TRCSEQEVR<n>, Sequencer State Transition Control Register <n> , n = 0 - 2](#) on page 2119 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-385: AARCH64\_TRCSEQEVR&lt;n&gt; bit assignments

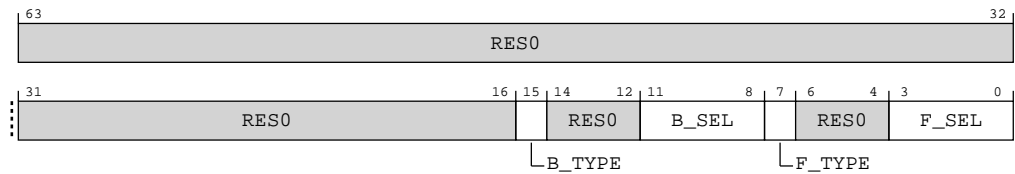


Table A-982: TRCSEQEVR&lt;n&gt; bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0
[15]	B_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Backward field. Defines whether the backward resource event is a single Resource Selector or a Resource Selector pair. When the resource event occurs then the sequencer state moves from state n+1 to state n. For example, if TRCSEQEVR2.B_SEL == 0x14 then when event 0x14 occurs, the sequencer moves from state 3 to state 2.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>B_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>B_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. B_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[14:12]	RES0	Reserved	RES0
[11:8]	B_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. B_TYPE controls whether B_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Backward field. Selects the single Resource Selector or Resource Selector pair.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

Bits	Name	Description	Reset
[7]	F_TYPE	Chooses the type of Resource Selector.  Forward field. Defines whether the forward resource event is a single Resource Selector or a Resource Selector pair. When the resource event occurs then the sequencer state moves from state n to state n+1. For example, if TRCSEQEVR1.F_SEL == 0x12 then when event 0x12 occurs, the sequencer moves from state 1 to state 2.  <b>0b0</b> A single Resource Selector.  F_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  F_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. F_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	F_SEL	Defines the selected Resource Selector or pair of Resource Selectors. F_TYPE controls whether F_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  Forward field. Selects the single Resource Selector or Resource Selector pair.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

### Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQEVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'00':m[1:0]	0b100

MSR TRCSEQEVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'00':m[1:0]	0b100

### Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQEVR<m>

```
integer m = UInt(CRm<1:0>);
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
```

```

    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSEQEVR[m];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCSEQEVR[m];

```

MSR TRCSEQEVR&lt;m&gt;, &lt;Xt&gt;

```

integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSEQEVR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSEQEVR[m] = X[t, 64];

```

### A.2.8.2 TRCCNTRLDVR<n>, Counter Reload Value Register <n> , n = 0 - 1

This sets or returns the reload count value for counter <n>.

#### Configurations

AArch64 register TRCCNTRLDVR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.23 TRCCNTRLDVR<n>, Counter Reload Value Register <n> , n = 0 - 1](#) on page 2126 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-386: AARCH64\_TRCCNTRLDVR<n> bit assignments

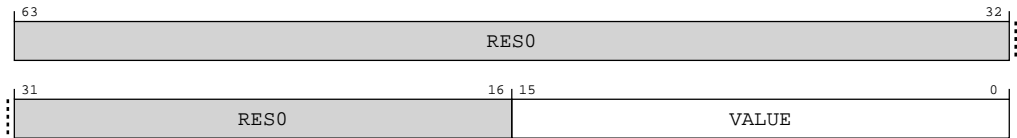


Table A-985: TRCCNTRLDVR<n> bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0
[15:0]	VALUE	Contains the reload value for counter <n>. When a reload event occurs for counter <n> then the trace unit copies the VALUE<n> field into counter <n>.	16 {x}

Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

MRS <Xt>, TRCCNTRLDVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'00':m[1:0]	0b101

MSR TRCCNTRLDVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'00':m[1:0]	0b101

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

MRS <Xt>, TRCCNTRLDVR<m>

```
integer m = UInt(CRm<1:0>);  
  
if PSTATE.EL == EL0 then  
    UNDEFINED;  
elseif PSTATE.EL == EL1 then  
    if CPACR_EL1.TTA == '1' then  
        AArch64.SystemAccessTrap(EL1, 0x18);  
    elseif CPTR_EL2.TTA == '1' then  
        AArch64.SystemAccessTrap(EL2, 0x18);
```

```

    else
        X[t, 64] = TRCCNTRLDVR[m];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCCNTRLDVR[m];

```

MSR TRCCNTRLDVR&lt;m&gt;, &lt;Xt&gt;

```

integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTRLDVR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTRLDVR[m] = X[t, 64];

```

### A.2.8.3 TRCCNTCTLR<n>, Counter Control Register <n> , n = 0 - 1

Controls the operation of counter <n>.

#### Configurations

AArch64 register TRCCNTCTLR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.24 TRCCNTCTLR<n>, Counter Control Register <n> , n = 0 - 1](#) on page 2128 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-387: AARCH64\_TRCCNTCTLR<n> bit assignments

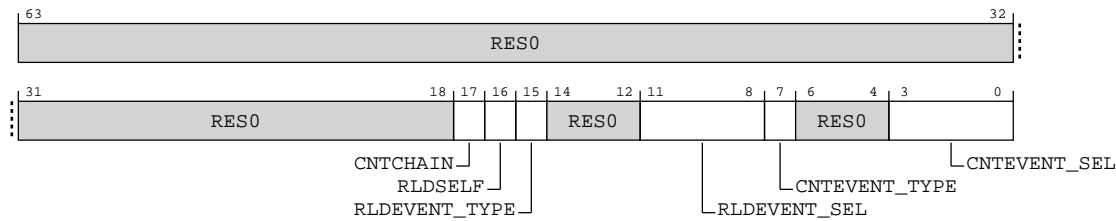


Table A-988: TRCCNTCTLR<n> bit descriptions

Bits	Name	Description	Reset
[63:18]	RES0	Reserved	RES0
[17]	CNTCHAIN	For TRCCNTCTLR1, this bit controls whether the counter decrements when a reload event occurs for counter <n-1>.  <b>0b0</b> The counter does not decrement when a reload event for counter <n-1> occurs.  <b>0b1</b> Counter <n> decrements when a reload event for counter <n-1> occurs. This concatenates counter <n> and counter <n-1>, to provide a larger count value.  CNTCHAIN is not implemented for TRCCNTCTLR0.	x
[16]	RLDSELF	Controls whether a reload event occurs for the counter, when the counter reaches zero.  <b>0b0</b> Normal mode.  The counter is in Normal mode.  <b>0b1</b> Self-reload mode.  The counter is in Self-reload mode.	x

Bits	Name	Description	Reset
[15]	RLDEVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Selects an event, that when it occurs causes a reload event for counter &lt;n&gt;.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>RLDEVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>RLDEVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. RLDEVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[14:12]	RES0	Reserved	RES0
[11:8]	RLDEVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. RLDEVENT_TYPE controls whether RLDEVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Selects an event, that when it occurs causes a reload event for counter &lt;n&gt;.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx
[7]	CNTEVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Selects an event, that when it occurs causes counter &lt;n&gt; to decrement.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>CNTEVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>CNTEVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. CNTEVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[6:4]	RES0	Reserved	RES0
[3:0]	CNTEVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. CNTEVENT_TYPE controls whether CNTEVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Selects an event, that when it occurs causes counter &lt;n&gt; to decrement.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

## Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.



MRS &lt;Xt&gt;, TRCCNTCTLR&lt;m&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'01':m[1:0]	0b101

MSR TRCCNTCTLR&lt;m&gt;, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'01':m[1:0]	0b101

## Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

MRS &lt;Xt&gt;, TRCCNTCTLR&lt;m&gt;

```
integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCNTCTLR[m];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCNTCTLR[m];
```

MSR TRCCNTCTLR&lt;m&gt;, &lt;Xt&gt;

```
integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTCTLR[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTCTLR[m] = X[t, 64];
```

A.2.8.4 TRCCNTVR<n>, Counter Value Register <n> , n = 0 - 1

This sets or returns the value of counter <n>.

Configurations

AArch64 register TRCCNTVR<n> bits [31:0] are architecturally mapped to External register B.2.2.7.25 TRCCNTVR<n>, Counter Value Register <n> , n = 0 - 1 on page 2131 bits [31:0].

Attributes

Width

64

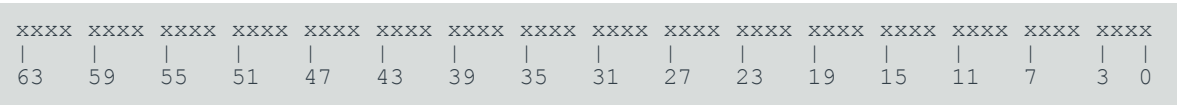
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-388: AARCH64\_TRCCNTVR<n> bit assignments

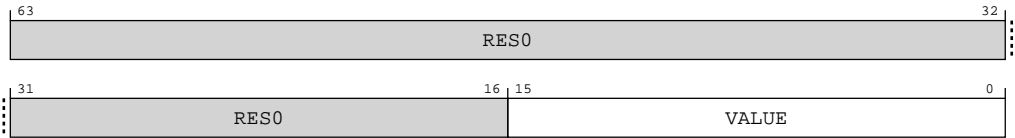


Table A-991: TRCCNTVR<n> bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0
[15:0]	VALUE	Contains the count value of counter.	16 {x}

Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

MRS &lt;Xt&gt;, TRCCNTVR&lt;m&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'10':m[1:0]	0b101

MSR TRCCNTVR&lt;m&gt;, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	'10':m[1:0]	0b101

## Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

MRS &lt;Xt&gt;, TRCCNTVR&lt;m&gt;

```
integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCNTVR[m];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCNTVR[m];
```

MSR TRCCNTVR&lt;m&gt;, &lt;Xt&gt;

```
integer m = UInt(CRm<1:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTVR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCNTVR[m] = X[t, 64];
```

A.2.8.5 TRCTRACEIDR, Trace ID Register

Sets the trace ID for instruction trace.

Configurations

AArch64 register TRCTRACEIDR bits [31:0] are architecturally mapped to External register [B.2.2.7.12 TRCTRACEIDR, Trace ID Register](#) on page 2104 bits [31:0].

Attributes

Width

64

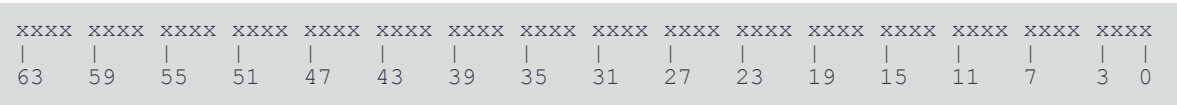
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-389: AARCH64\_TRCTRACEIDR bit assignments

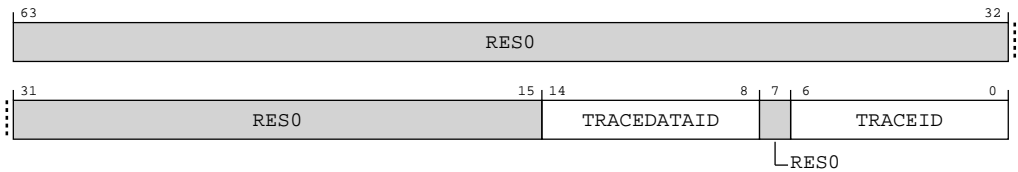


Table A-994: TRCTRACEIDR bit descriptions

Bits	Name	Description	Reset
[63:15]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[14:8]	TRACEDATAID	Data Trace ID.  Sets the trace ID value for data trace.  Writing a reserved trace ID value does not affect behavior of the trace unit but it might cause <b>UNPREDICTABLE</b> behavior of the trace capture infrastructure.  See the AMBA ATB Protocol Specification for information about which ATID values are reserved.	7{x}
[7]	RES0	Reserved	RES0
[6:0]	TRACEID	Trace ID.  Sets the trace ID value for instruction trace.  Writing a reserved trace ID value does not affect behavior of the trace unit but it might cause <b>UNPREDICTABLE</b> behavior of the trace capture infrastructure.  See the AMBA ATB Protocol Specification for information about which ATID values are reserved.	7{x}

### Access

Must be programmed if implemented.

MRS <Xt>, TRCTRACEIDR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b001

MSR TRCTRACEIDR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b001

### Accessibility

Must be programmed if implemented.

MRS <Xt>, TRCTRACEIDR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCTRACEIDR;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCTRACEIDR;

```

MSR TRCTRACEIDR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCTRACEIDR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCTRACEIDR = X[t, 64];
```

A.2.8.6 TRCVICTLR, ViewInst Main Control Register

Controls instruction trace filtering.

Configurations

AArch64 register TRCVICTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.13 TRCVICTLR, ViewInst Main Control Register](#) on page 2105 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

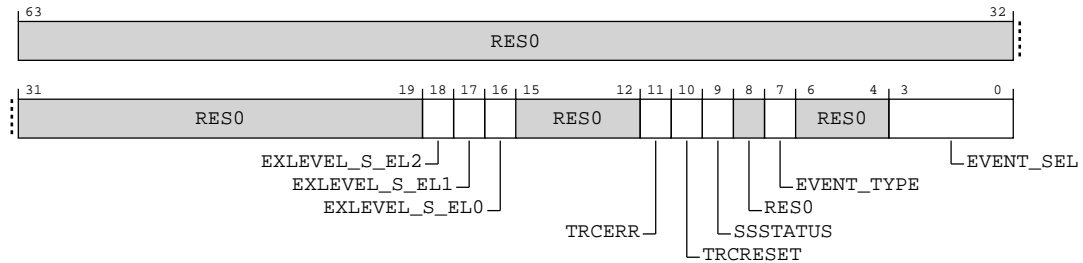
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-390: AARCH64\_TRCVICTLR bit assignments**



**Table A-997: TRCVICTLR bit descriptions**

Bits	Name	Description	Reset
[63:19]	RES0	Reserved	RES0
[18]	EXLEVEL_S_EL2	Filter instruction trace for EL2 in Secure state. <b>0b0</b> The trace unit generates instruction trace for EL2 in Secure state. <b>0b1</b> The trace unit does not generate instruction trace for EL2 in Secure state.	x
[17]	EXLEVEL_S_EL1	Filter instruction trace for EL1 in Secure state. <b>0b0</b> The trace unit generates instruction trace for EL1 in Secure state. <b>0b1</b> The trace unit does not generate instruction trace for EL1 in Secure state.	x
[16]	EXLEVEL_S_ELO	Filter instruction trace for ELO in Secure state. <b>0b0</b> The trace unit generates instruction trace for ELO in Secure state. <b>0b1</b> The trace unit does not generate instruction trace for ELO in Secure state.	x
[15:12]	RES0	Reserved	RES0
[11]	TRCERR	Controls the forced tracing of System Error exceptions. <b>0b0</b> Forced tracing of System Error exceptions is disabled. <b>0b1</b> Forced tracing of System Error exceptions is enabled.	x
[10]	TRCRESET	Controls the forced tracing of PE Resets. <b>0b0</b> Forced tracing of PE Resets is disabled. <b>0b1</b> Forced tracing of PE Resets is enabled.	x

Bits	Name	Description	Reset
[9]	SSSTATUS	<p>ViewInst start/stop function status.</p> <p><b>0b0</b></p> <p>Stopped State.</p> <p>The ViewInst start/stop function is in the stopped state.</p> <p><b>0b1</b></p> <p>Started State.</p> <p>The ViewInst start/stop function is in the started state.</p> <p>Before software enables the trace unit, it must write to this bit to set the initial state of the ViewInst start/stop function. If the ViewInst start/stop function is not used then set this bit to 0b1. Arm recommends that the value of this bit is set before each trace session begins.</p> <p>If the trace unit becomes disabled while a start point or stop point is still speculative, then the value of SSSTATUS is <b>UNKNOWN</b> and might represent the result of a speculative start point or stop point.</p> <p>If software which is running on the PE being traced disables the trace unit, either by clearing AArch64-TRCPRGCTLR.EN or locking the OS Lock, Arm recommends that a DSB and an ISB instruction are executed before disabling the trace unit to prevent any start points or stop points being speculative at the point of disabling the trace unit. This procedure assumes that all start points or stop points occur before the barrier instructions are executed. The procedure does not guarantee that there are no speculative start points or stop points when disabling, although it helps minimize the probability.</p>	x
[8]	RES0	Reserved	RES0
[7]	EVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

## Access

Must be programmed.

MRS <Xt>, TRCVICTLR



op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b010

MSR TRCVICTLR, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b010

### Accessibility

Must be programmed.

MRS &lt;Xt&gt;, TRCVICTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVICTLR;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVICTLR;

```

MSR TRCVICTLR, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVICTLR = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVICTLR = X[t, 64];

```

### A.2.8.7 TRCIDR8, ID Register 8

Returns the maximum speculation depth of the instruction trace element stream.

### Configurations

AArch64 register TRCIDR8 bits [31:0] are architecturally mapped to External register [B.2.2.7.26 TRCIDR8, ID Register 8](#) on page 2132 bits [31:0].

## Attributes

## Width

64

## Functional group

## Trace unit registers

## Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



### Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure A-391: AARCH64\_TRCIDR8 bit assignments

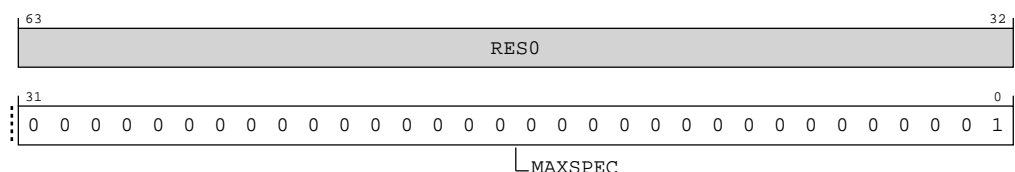


Table A-1000: TRCIDR8 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	MAXSPEC	Indicates the maximum speculation depth of the instruction trace element stream. This is the maximum number of PO elements in the trace element stream that can be speculative at any time.  <b>0b00000000000000000000000000000001</b> 1 speculative PO element.	0x00000001

## Access

MRS &lt;Xt&gt;, TRCIDR8

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b110

Accessibility

MRS <Xt>, TRCIDR8

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR8;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR8;
```

A.2.8.8 TRCIMSPECO, IMP DEF Register 0

TRCIMSPECO shows the presence of any **IMPLEMENTATION DEFINED** features, and provides an interface to enable the features that are provided.

Configurations

AArch64 register TRCIMSPECO bits [31:0] are architecturally mapped to External register [B.2.2.7.32 TRCIMSPECO, IMP DEF Register 0](#) on page 2138 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-392: AARCH64\_TRCIMSPECO bit assignments

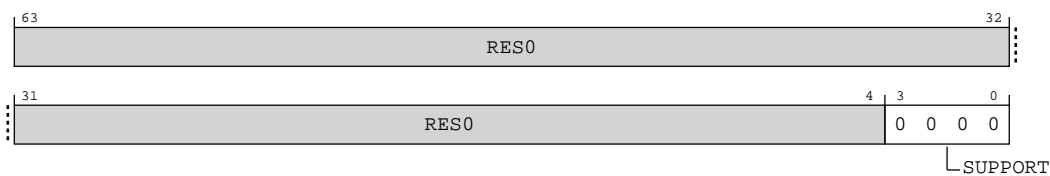


Table A-1002: TRCIMSPECO bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	SUPPORT	Indicates whether the implementation supports <b>IMPLEMENTATION DEFINED</b> features.  <b>0b0000</b> No <b>IMPLEMENTATION DEFINED</b> features are supported.	0b0000

Access

MRS <Xt>, TRCIMSPECO

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b111

MSR TRCIMSPECO, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0000	0b111

Accessibility

MRS <Xt>, TRCIMSPECO

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIMSPECO;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIMSPECO;
```

MSR TRCIMSPECO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
```

```
elseif PSTATE.EL == EL1 then
  if CPACR_EL1.TTA == '1' then
    AArch64.SystemAccessTrap(EL1, 0x18);
  elseif CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    TRCIMSPEC0 = X[t, 64];
elseif PSTATE.EL == EL2 then
  if CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    TRCIMSPEC0 = X[t, 64];
```

A.2.8.9 TRCPRGCTLR, Programming Control Register

Enables the trace unit.

Configurations

AArch64 register TRCPRGCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.1 TRCPRGCTLR, Programming Control Register](#) on page 2081 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

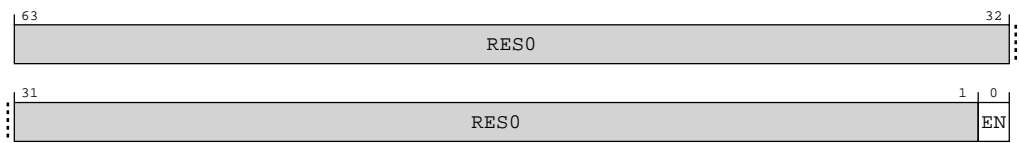
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-393: AARCH64\_TRCPRGCTLR bit assignments



**Table A-1005: TRCPRGCTLR bit descriptions**

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	EN	Trace unit enable.  <b>0b0</b> The trace unit is disabled.  <b>0b1</b> The trace unit is enabled.	0b0

**Access**

Must be programmed.

MRS <Xt>, TRCPRGCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0001	0b000

MSR TRCPRGCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0001	0b000

**Accessibility**

Must be programmed.

MRS <Xt>, TRCPRGCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCPRGCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCPRGCTLR;

```

MSR TRCPRGCTLR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCPRGCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then

```

```
if CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    TRCPRGCTLR = X[t, 64];
```

A.2.8.10 TRCVIIECTLR, ViewInst Include/Exclude Control Register

Use this to select, or read, the Address Range Comparators for the ViewInst include/exclude function.

Configurations

AArch64 register TRCVIIECTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.14 TRCVIIECTLR, ViewInst Include/Exclude Control Register](#) on page 2108 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

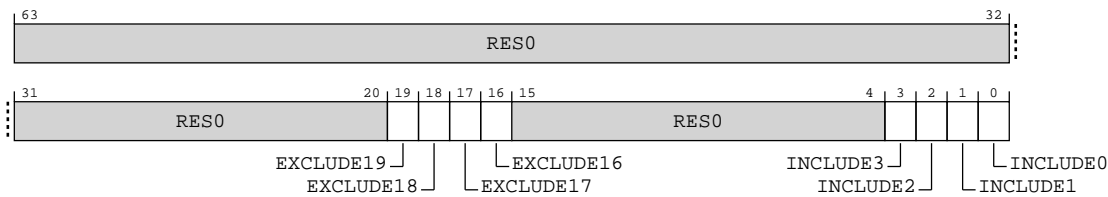
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-394: AARCH64\_TRCVIIECTLR bit assignments



**Table A-1008: TRCVIIECTLR bit descriptions**

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0
[19:16]	EXCLUDE<m>, bit[m], where m = 19 to 16	<p>Selects which Address Range Comparators are in use with the ViewInst exclude function.</p> <p>Each bit represents an Address Range Comparator, so bit[m] controls the selection of Address Range Comparator m.</p> <p><b>0b0</b></p> <p>The address range that Address Range Comparator m defines, is not selected for the ViewInst exclude function.</p> <p><b>0b1</b></p> <p>The address range that Address Range Comparator m defines, is selected for the ViewInst exclude function.</p>	xxxx
[15:4]	RES0	Reserved	RES0
[3:0]	INCLUDE<m>, bit[m], where m = 3 to 0	<p>Selects which Address Range Comparators are in use with the ViewInst include function.</p> <p>Each bit represents an Address Range Comparator, so bit[m] controls the selection of Address Range Comparator m.</p> <p>Selecting no comparators for the ViewInst include function indicates that all instructions are included by default.</p> <p>The ViewInst exclude function then indicates which ranges are excluded.</p> <p><b>0b0</b></p> <p>The address range that Address Range Comparator m defines, is not selected for the ViewInst include function.</p> <p><b>0b1</b></p> <p>The address range that Address Range Comparator m defines, is selected for the ViewInst include function.</p>	xxxx

### Access

Must be programmed if AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

MRS <Xt>, TRCVIIECTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0001	0b010

MSR TRCVIIECTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0001	0b010

### Accessibility

Must be programmed if AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

MRS <Xt>, TRCVIIECTLR

```
if PSTATE.EL == EL0 then
```



```

    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVIIECTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVIIECTLR;

```

MSR TRCVIIECTLR, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVIIECTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVIIECTLR = X[t, 64];

```

### A.2.8.11 TRCIDR9, ID Register 9

Returns the tracing capabilities of the trace unit.

#### Configurations

AArch64 register TRCIDR9 bits [31:0] are architecturally mapped to External register [B.2.2.7.27 TRCIDR9, ID Register 9](#) on page 2133 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0010	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-395: AARCH64\_TRCIDR9 bit assignments

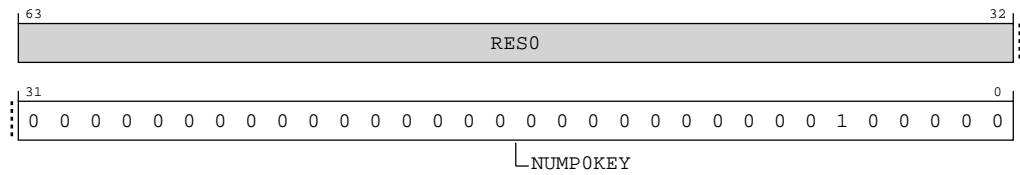


Table A-1011: TRCIDR9 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	NUMPOKEY	Indicates the number of PO right-hand keys.  0b0000000000000000000000000000000100000 32 PO right-hand keys.	0x00000020

Access

MRS <Xt>, TRCIDR9

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0001	0b110

Accessibility

MRS <Xt>, TRCIDR9

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR9;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR9;
```

A.2.8.12 TRCVISSCTLR, ViewInst Start/Stop Control Register

Use this to select, or read, the Single Address Comparators for the ViewInst start/stop function.

Configurations

AArch64 register TRCVISSCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.15 TRCVISSCTLR, ViewInst Start/Stop Control Register](#) on page 2110 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-396: AARCH64\_TRCVISSCTLR bit assignments

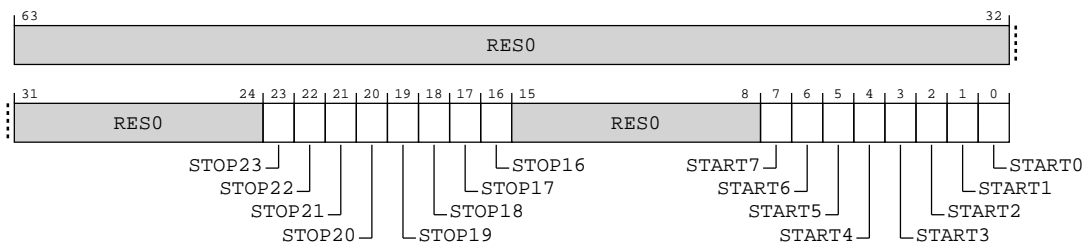


Table A-1013: TRCVISSCTLR bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[23:16]	STOP<m>, bit[m], where m = 23 to 16	<p>Selects which Single Address Comparators are in use with ViewInst start/stop function, for the purpose of stopping trace.</p> <p><b>0b0</b> The Single Address Comparator m, is not selected as a stop resource.</p> <p><b>0b1</b> The Single Address Comparator m, is selected as a stop resource.</p>	8 {x}
[15:8]	RES0	Reserved	RES0
[7:0]	START<m>, bit[m], where m = 7 to 0	<p>Selects which Single Address Comparators are in use with ViewInst start/stop function, for the purpose of starting trace.</p> <p><b>0b0</b> The Single Address Comparator m, is not selected as a start resource.</p> <p><b>0b1</b> The Single Address Comparator m, is selected as a start resource.</p>	8 {x}

## Access

Must be programmed if AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

For any 2 comparators selected for the ViewInst start/stop function, the comparator containing the lower address must be a lower numbered comparator.

MRS <Xt>, TRCVISSCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0010	0b010

MSR TRCVISSCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0010	0b010

## Accessibility

Must be programmed if AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

For any 2 comparators selected for the ViewInst start/stop function, the comparator containing the lower address must be a lower numbered comparator.

MRS <Xt>, TRCVISSCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVISSCTLR;
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);

```

```
else
    X[t, 64] = TRCVISSCTLR;
```

MSR TRCVISSCTLR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVISSCTLR = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVISSCTLR = X[t, 64];
```

A.2.8.13 TRCIDR10, ID Register 10

Returns the tracing capabilities of the trace unit.

Configurations

AArch64 register TRCIDR10 bits [31:0] are architecturally mapped to External register [B.2.2.7.28 TRCIDR10, ID Register 10](#) on page 2134 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	1000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Attributes

Width

64

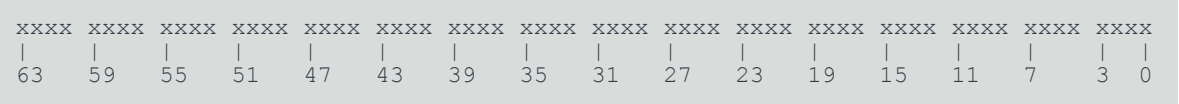
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-398: AARCH64\_TRCSTATR bit assignments

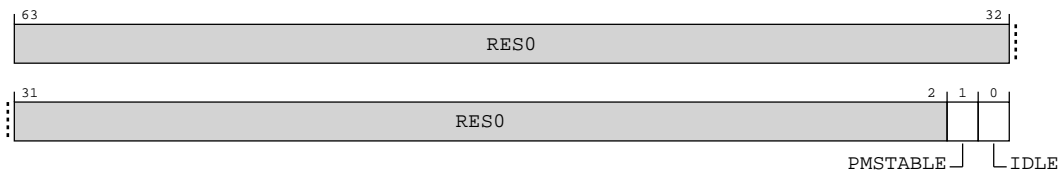


Table A-1018: TRCSTATR bit descriptions

Bits	Name	Description	Reset
[63:2]	RES0	Reserved	RES0
[1]	PMSTABLE	Programmers' model stable.  <b>0b0</b> The programmers' model is not stable.  <b>0b1</b> The programmers' model is stable.  This bit is <b>UNKNOWN</b> while the trace unit is enabled.	x
[0]	IDLE	Idle status.  <b>0b0</b> The trace unit is not idle.  <b>0b1</b> The trace unit is idle.	x

Access

MRS <Xt>, TRCSTATR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0011	0b000

Accessibility

MRS <Xt>, TRCSTATR

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSTATR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSTATR;
```

A.2.8.15 TRCIDR11, ID Register 11

Returns the tracing capabilities of the trace unit.

**Configurations**

AArch64 register TRCIDR11 bits [31:0] are architecturally mapped to External register [B.2.2.7.29 TRCIDR11, ID Register 11](#) on page 2135 bits [31:0].

**Attributes**

**Width**

64

**Functional group**

Trace unit registers

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-399: AARCH64\_TRCIDR11 bit assignments

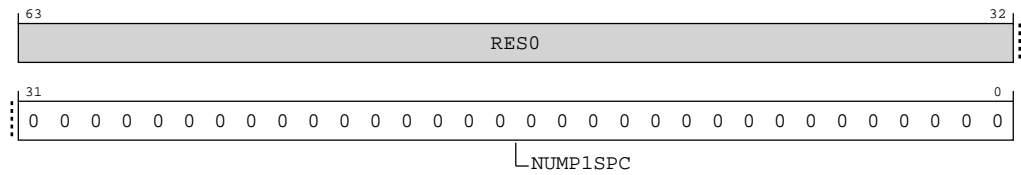


Table A-1020: TRCIDR11 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	NUMP1SPC	Indicates the number of special P1 right-hand keys.  0b00000000000000000000000000000000 No special P1 right-hand keys.	0x00000000

Access

MRS <Xt>, TRCIDR11

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0011	0b110

Accessibility

MRS <Xt>, TRCIDR11

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR11;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR11;
```

A.2.8.16 TRCCONFIGR, Trace Configuration Register

Controls the tracing options.

Configurations

AArch64 register TRCCONFIGR bits [31:0] are architecturally mapped to External register [B.2.2.7.3 TRCCONFIGR, Trace Configuration Register](#) on page 2084 bits [31:0].

Attributes

Width

64

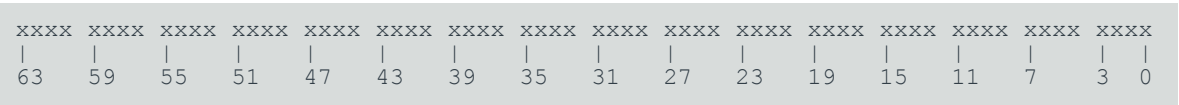
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-400: AARCH64\_TRCCONFIGR bit assignments

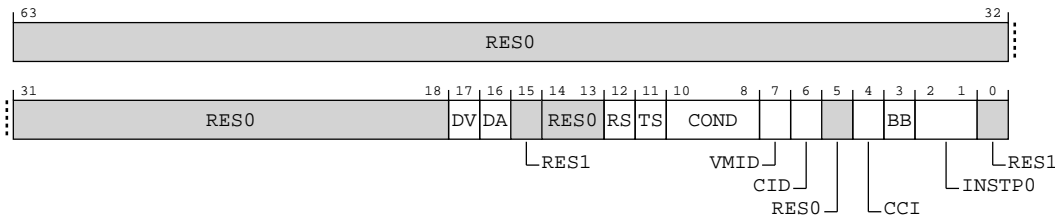


Table A-1022: TRCCONFIGR bit descriptions

Bits	Name	Description	Reset
[63:18]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[17]	DV	Data value tracing bit.  <b>0b0</b> Data value tracing is disabled.  <b>0b1</b> Data value tracing is enabled when INSTP0 is not 0b00.	x
[16]	DA	Data address tracing bit.  <b>0b0</b> Data address tracing is disabled.  <b>0b1</b> Data address tracing is enabled when INSTP0 is not 0b00.	x
[15]	RES1	Reserved	RES1
[14:13]	RES0	Reserved	RES0
[12]	RS	Return stack control.  <b>0b0</b> Return stack is disabled.  <b>0b1</b> Return stack is enabled.	x
[11]	TS	Global timestamp tracing control.  <b>0b0</b> Global timestamp tracing is disabled.  <b>0b1</b> Global timestamp tracing is enabled.	x
[10:8]	COND	Conditional instruction tracing bit. The permitted values are:  <b>0b000</b> Conditional instruction tracing is disabled.  <b>0b001</b> Conditional load instructions are traced.  <b>0b010</b> Conditional store instructions are traced.  <b>0b011</b> Conditional load and store instructions are traced.  <b>0b111</b> All conditional instructions are traced.	xxx
[7]	VMID	Virtual context identifier tracing control.  <b>0b0</b> Virtual context identifier tracing is disabled.  <b>0b1</b> Virtual context identifier tracing is enabled.	x

Bits	Name	Description	Reset
[6]	CID	Context identifier tracing control.  <b>0b0</b> Context identifier tracing is disabled.  <b>0b1</b> Context identifier tracing is enabled.	x
[5]	RES0	Reserved	RES0
[4]	CCI	Cycle counting instruction tracing control.  <b>0b0</b> Cycle counting instruction tracing is disabled.  <b>0b1</b> Cycle counting instruction tracing is enabled.	x
[3]	BB	Branch broadcasting control.  <b>0b0</b> Branch broadcasting is disabled.  <b>0b1</b> Branch broadcasting is enabled.	x
[2:1]	INSTPO	Instruction P0 field. This field controls whether load and store instructions are traced as P0 instructions:  <b>0b00</b> Do not trace load and store instructions as P0 instructions.  <b>0b01</b> Trace load instructions as P0 instructions.  <b>0b10</b> Trace store instructions as P0 instructions.  <b>0b11</b> Trace load and store instructions as P0 instructions.	xx
[0]	RES1	Reserved	RES1

## Access

Must always be programmed.

TRCCONFIGR.QE must be set to 0b00 if TRCCONFIGR.BB is not 0b0.

MRS <Xt>, TRCCONFIGR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0100	0b000

MSR TRCCONFIGR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0100	0b000

## Accessibility

Must always be programmed.

TRCCONFIGR.QE must be set to 0b00 if TRCCONFIGR.BB is not 0b0.

MRS <Xt>, TRCCONFIGR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCONFIGR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCONFIGR;

```

MSR TRCCONFIGR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCONFIGR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCONFIGR = X[t, 64];

```

### A.2.8.17 TRCIDR12, ID Register 12

Returns the tracing capabilities of the trace unit.

## Configurations

AArch64 register TRCIDR12 bits [31:0] are architecturally mapped to External register [B.2.2.7.30 TRCIDR12, ID Register 12](#) on page 2136 bits [31:0].

## Attributes

### Width

64

### Functional group

Trace unit registers

### Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure A-401: AARCH64\_TRCIDR12 bit assignments

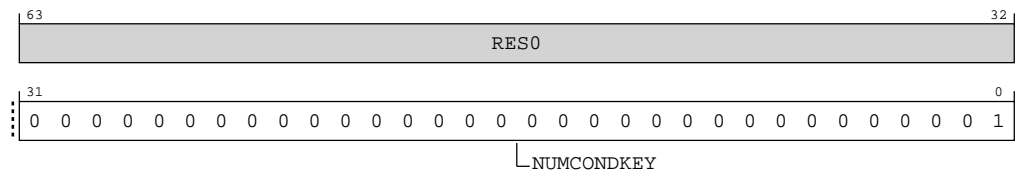


Table A-1025: TRCIDR12 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	NUMCONDKEY	Indicates the number of conditional instruction right-hand keys.  0b00000000000000000000000000000001 1 conditional instruction right-hand key.	0x00000001

## Access

MRS &lt;Xt&gt;, TRCIDR12

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0100	0b110

## Accessibility

MRS &lt;Xt&gt;, TRCIDR12

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR12;
    end
end

```

```
elseif PSTATE.EL == EL2 then
  if CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    X[t, 64] = TRCIDR12;
```

A.2.8.18 TRCIDR13, ID Register 13

Returns the tracing capabilities of the trace unit.

Configurations

AArch64 register TRCIDR13 bits [31:0] are architecturally mapped to External register [B.2.2.7.31 TRCIDR13, ID Register 13](#) on page 2137 bits [31:0].

Attributes

Width

64

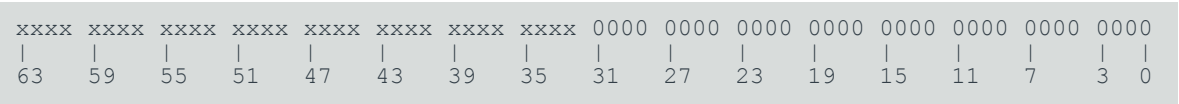
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-402: AARCH64\_TRCIDR13 bit assignments

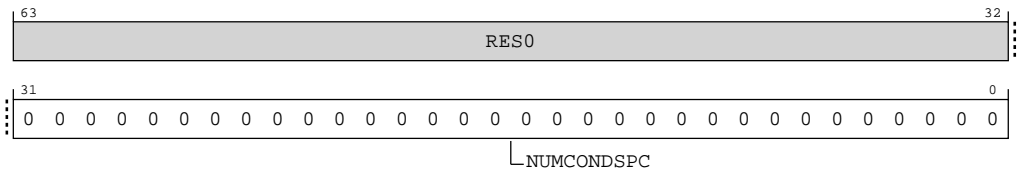


Table A-1027: TRCIDR13 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:0]	NUMCONDSPC	Indicates the number of special conditional instruction right-hand keys.  <b>0b00000000000000000000000000000000</b> No special conditional instruction right-hand keys.	0x00000000

**Access**  
MRS <Xt>, TRCIDR13

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0101	0b110

**Accessibility**  
MRS <Xt>, TRCIDR13

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR13;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR13;
```

A.2.8.19 TRCAUXCTLR, Auxillary Control Register

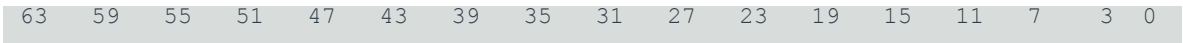
Trace micro-architectural control bits.

**Configurations**  
AArch64 register TRCAUXCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.4 TRCAUXCTLR, Auxillary Control Register](#) on page 2087 bits [31:0].

**Attributes**  
**Width**  
64  
**Functional group**  
Trace unit registers  
**Access type**  
See bit descriptions  
**Reset value**







Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-403: AARCH64\_TRCAUXCTLR bit assignments

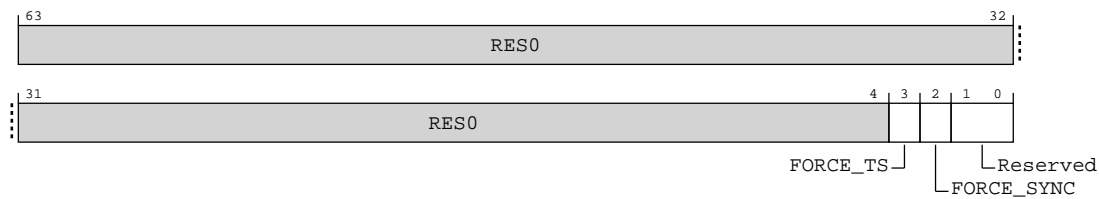


Table A-1029: TRCAUXCTLR bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3]	FORCE_TS	Force overflow when no timestamp is generated between two trace info packets.  0b0 Force overflow disabled.  0b1 Force overflow enabled.	0b0
[2]	FORCE_SYNC	Force overflow when the generation of trace synchronisation packets is delayed.  0b0 Force overflow disabled.  0b1 Force overflow enabled.	0b0
[1:0]	Reserved	Trace unit control options which are reserved for Arm internal use.  0b00 Any trace unit control options affected by this register are disabled.  All other values are reserved for Arm internal use. Arm strongly recommends that you do not modify this field unless directed by Arm.	0b00

Access

If this register is set to nonzero then it might cause the behavior of a trace unit to contradict the architecture specification. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, TRCAUXCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0110	0b000

MSR TRCAUXCTLR, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0110	0b000

### Accessibility

If this register is set to nonzero then it might cause the behavior of a trace unit to contradict the architecture specification. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS &lt;Xt&gt;, TRCAUXCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCAUXCTLR;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCAUXCTLR;

```

MSR TRCAUXCTLR, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCAUXCTLR = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCAUXCTLR = X[t, 64];

```

### A.2.8.20 TRCSEQRSTEV, Sequencer Reset Control Register

Moves the sequencer to state 0 when a programmed resource event occurs.

#### Configurations

AArch64 register TRCSEQRSTEV bits [31:0] are architecturally mapped to External register

[B.2.2.7.20 TRCSEQRSTEV, Sequencer Reset Control Register](#) on page 2122 bits [31:0].

Attributes

Width

64

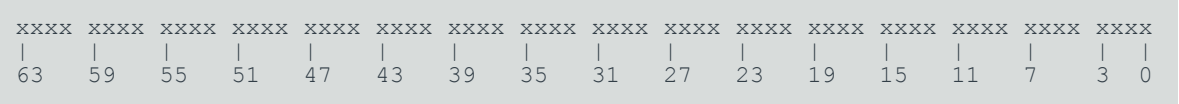
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-404: AARCH64\_TRCSEQRSTEVR bit assignments

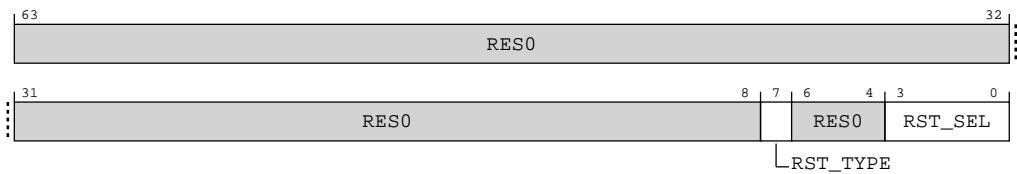


Table A-1032: TRCSEQRSTEVR bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7]	RST_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  RST_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  RST_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. RST_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3:0]	RST_SEL	Defines the selected Resource Selector or pair of Resource Selectors. RST_TYPE controls whether RST_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

### Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQRSTEV

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0110	0b100

MSR TRCSEQRSTEV, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0110	0b100

### Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQRSTEV

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSEQRSTEV;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSEQRSTEV;

```

MSR TRCSEQRSTEV, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSEQRSTEV = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);

```

```
else
    TRCSEQRSTEVr = X[t, 64];
```

A.2.8.21 TRCSEQSTR, Sequencer State Register

Use this to set, or read, the sequencer state.

Configurations

AArch64 register TRCSEQSTR bits [31:0] are architecturally mapped to External register [B.2.2.7.21 TRCSEQSTR, Sequencer State Register](#) on page 2123 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-405: AARCH64\_TRCSEQSTR bit assignments

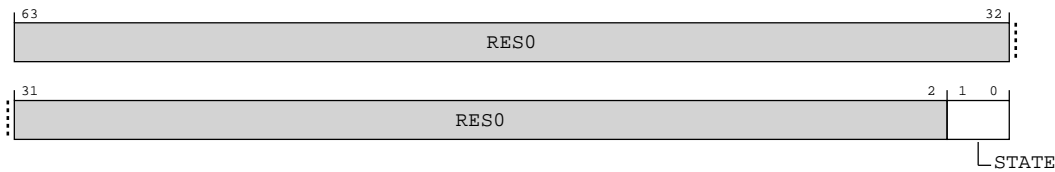


Table A-1035: TRCSEQSTR bit descriptions

Bits	Name	Description	Reset
[63:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1:0]	STATE	Set or returns the state of the sequencer.  <b>0b00</b> State 0.  <b>0b01</b> State 1.  <b>0b10</b> State 2.  <b>0b11</b> State 3.	xx

### Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQSTR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0111	0b100

MSR TRCSEQSTR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b0111	0b100

### Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

MRS <Xt>, TRCSEQSTR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSEQSTR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSEQSTR;

```

MSR TRCSEQSTR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then

```

```
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSEQSTR = X[t, 64];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            TRCSEQSTR = X[t, 64];
```

A.2.8.22 TRCEVENTCTLOR, Event Control 0 Register

Controls the generation of tracing events.

Configurations

AArch64 register TRCEVENTCTLOR bits [31:0] are architecturally mapped to External register [B.2.2.7.5 TRCEVENTCTLOR, Event Control 0 Register](#) on page 2089 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-406: AARCH64\_TRCEVENTCTL0R bit assignments

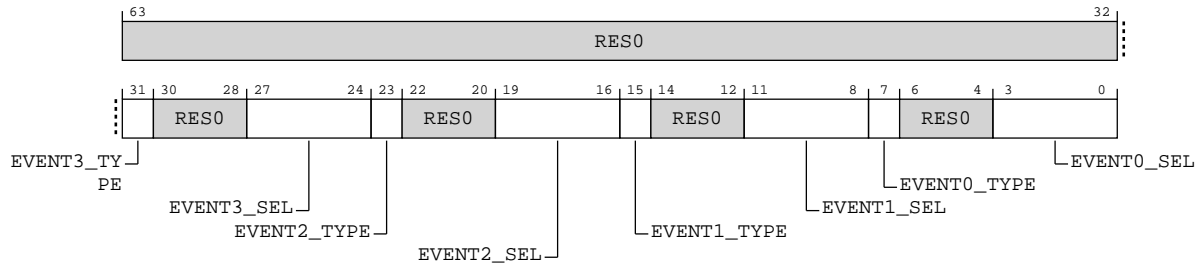


Table A-1038: TRCEVENTCTL0R bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	EVENT3_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT3_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT3_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT3_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[30:28]	RES0	Reserved	RES0
[27:24]	EVENT3_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT3_TYPE controls whether EVENT3_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and AArch64-TRCEVENTCTL1R.INSTEN[3] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx
[23]	EVENT2_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT2_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT2_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT2_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x



Bits	Name	Description	Reset
[22:20]	<b>RES0</b>	Reserved	<b>RES0</b>
[19:16]	EVENT2_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT2_TYPE controls whether EVENT2_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and AArch64-TRCEVENTCTL1R.INSTEN[2] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx
[15]	EVENT1_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT1_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT1_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT1_SEL[3] is <b>RES0</b>.</p>	x
[14:12]	<b>RES0</b>	Reserved	<b>RES0</b>
[11:8]	EVENT1_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT1_TYPE controls whether EVENT1_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and AArch64-TRCEVENTCTL1R.INSTEN[1] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx
[7]	EVENT0_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT0_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT0_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT0_SEL[3] is <b>RES0</b>.</p>	x
[6:4]	<b>RES0</b>	Reserved	<b>RES0</b>
[3:0]	EVENT0_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT0_TYPE controls whether EVENT0_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and AArch64-TRCEVENTCTL1R.INSTEN[0] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx

Access

Must be programmed if implemented.

MRS <Xt>, TRCEVENTCTLOR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b000

MSR TRCEVENTCTLOR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b000

Accessibility

Must be programmed if implemented.

MRS <Xt>, TRCEVENTCTLOR

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEVENTCTLOR;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEVENTCTLOR;
```

MSR TRCEVENTCTLOR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCEVENTCTLOR = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCEVENTCTLOR = X[t, 64];
```

### A.2.8.23 TRCVDCTLR, ViewData Main Control Register

Controls data trace filtering.

## Configurations

AArch64 register TRCVDCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.16 TRCVDCTLR, ViewData Main Control Register](#) on page 2112 bits [31:0].

## Attributes

## Width

64

## Functional group

## Trace unit registers

### Access type

See bit descriptions

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

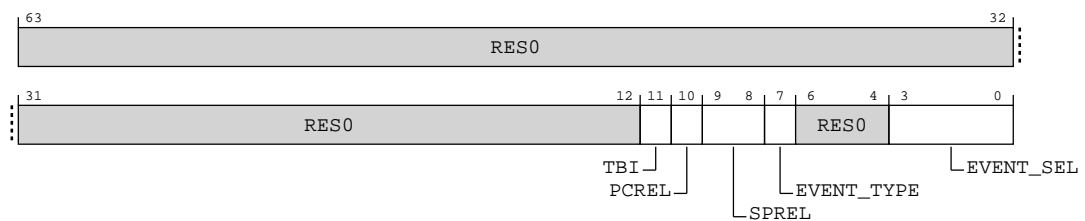


### Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure A-407: AARCH64\_TRCVDCTLR bit assignments



### Table A-1041: TRCVDCTLR bit descriptions

Bits	Name	Description	Reset
[63:12]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[11]	TBI	Controls which information a trace unit populates in bits[63:56] of the data address.  <b>0b0</b> The trace unit assigns bits[63:56] to have the same value as bit[55] of the data address, that is, it sign-extends the value.  <b>0b1</b> The trace unit assigns bits[63:56] to have the same value as bits[63:56] of the data address.	x
[10]	PCREL	Controls whether a trace unit traces data for transfers that are relative to the Program Counter (PC).  <b>0b0</b> The trace unit does not affect the tracing of PC-relative transfers.  <b>0b1</b> The trace unit does not trace the address or value portions of PC-relative transfers.  This bit only affects PC-relative transfers that use the PC as a base register plus an immediate offset.	x
[9:8]	SPREL	Controls whether a trace unit traces data for transfers that are relative to the Stack Pointer (SP).  <b>0b00</b> The trace unit does not affect the tracing of SP-relative transfers.  <b>0b01</b> Reserved.  <b>0b10</b> The trace unit does not trace the address portion of SP-relative transfers. If data value tracing is enabled then the trace unit generates a P1 data address element.  <b>0b11</b> The trace unit does not trace the address or value portions of SP-relative transfers.	xx
[7]	EVENT_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

## Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when data tracing is enabled, that is, when either AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.

MRS <Xt>, TRCVDCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b010

MSR TRCVDCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b010

## Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when data tracing is enabled, that is, when either AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.

MRS <Xt>, TRCVDCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDCTLR;

```

MSR TRCVDCTLR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDCTLR = X[t, 64];

```

A.2.8.24 TRCEXTINSELR, External Input Select Register

Use this to set, or read, which external inputs are resources to the trace unit.

Configurations

AArch64 register TRCEXTINSELR bits [31:0] are architecturally mapped to External register [B.2.2.7.22 TRCEXTINSELR, External Input Select Register](#) on page 2125 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-408: AARCH64\_TRCEXTINSELR bit assignments

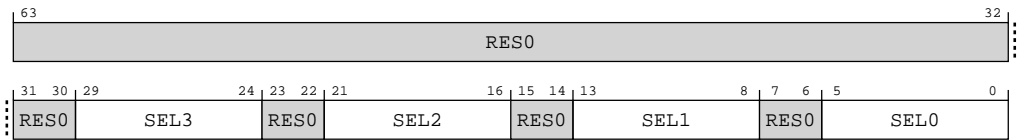


Table A-1044: TRCEXTINSELR bit descriptions

Bits	Name	Description	Reset
[63:30]	RES0	Reserved	RES0
[29:24]	SEL3	Selects external input resource #3.	6 { x }
[23:22]	RES0	Reserved	RES0
[21:16]	SEL2	Selects external input resource #2.	6 { x }
[15:14]	RES0	Reserved	RES0
[13:8]	SEL1	Selects external input resource #1.	6 { x }
[7:6]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[5:0]	SELO	Selects external input resource #0.	6{x}

## Access

Might ignore writes when the trace unit is enabled or not idle.

MRS <Xt>, TRCEXTINSEL

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b100

MSR TRCEXTINSEL, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b100

## Accessibility

Might ignore writes when the trace unit is enabled or not idle.

MRS <Xt>, TRCEXTINSEL

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEXTINSEL;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEXTINSEL;

```

MSR TRCEXTINSEL, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCEXTINSEL = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCEXTINSEL = X[t, 64];

```

A.2.8.25 TRCIDR0, ID Register 0

Returns the tracing capabilities of the trace unit.

Configurations

AArch64 register TRCIDR0 bits [31:0] are architecturally mapped to External register [B.2.2.7.33 TRCIDR0, ID Register 0](#) on page 2139 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	1000	xxxx	xx00	0x00	111x	1111	111x
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-409: AARCH64\_TRCIDR0 bit assignments

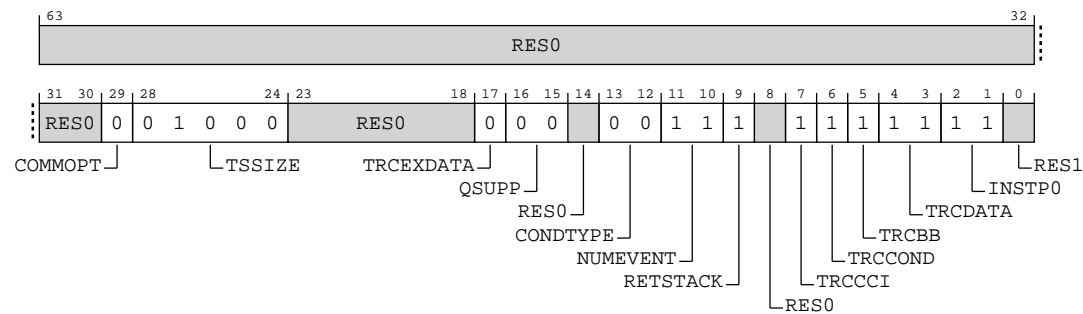


Table A-1047: TRCIDR0 bit descriptions

Bits	Name	Description	Reset
[63:30]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[29]	COMMOPT	Indicates how the commit field in Cycle count packets is interpreted.  <b>0b0</b> Commit mode 0.  Cycle count packets includes the Commit element to which the Cycle Count element is attached.	0b0
[28:24]	TSSIZE	Indicates that the trace unit implements Global timestamping and the size of the timestamp value.  <b>0b01000</b> Global timestamping implemented with a 64-bit timestamp value.	0b01000
[23:18]	RES0	Reserved	RES0
[17]	TRCEXDATA	Indicates if the trace unit implements tracing of data transfers for exceptions and exception returns.  <b>0b0</b> Tracing of data transfers for exceptions and exception returns not implemented.	0b0
[16:15]	QSUPP	Indicates that the trace unit implements Q element support.  <b>0b00</b> Q element support is not implemented.	0b00
[14]	RES0	Reserved	RES0
[13:12]	CONDTYPE	Indicates how conditional instructions are traced.  <b>0b00</b> Conditional instructions are traced with an indication of whether they pass or fail their condition code check.	0b00
[11:10]	NUMEVENT	Indicates the number of trace events implemented.  <b>0b11</b> The trace unit supports 4 trace events.	0b11
[9]	RETSTACK	Indicates if the trace unit supports the return stack.  <b>0b1</b> Return stack implemented.	0b1
[8]	RES0	Reserved	RES0
[7]	TRCCCI	Indicates if the trace unit implements cycle counting.  <b>0b1</b> Cycle counting implemented.	0b1
[6]	TRCCOND	Indicates if the trace unit implements conditional instruction tracing.  <b>0b1</b> Conditional instruction tracing implemented.	0b1
[5]	TRCBB	Indicates if the trace unit implements branch broadcasting.  <b>0b1</b> Branch broadcasting implemented.	0b1
[4:3]	TRCDATA	Indicates if the trace unit implements data tracing.  <b>0b11</b> Data tracing implemented.	0b11
[2:1]	INSTPO	Indicates if load and store instructions are PO instructions.  <b>0b11</b> Load and store instructions are PO instructions.	0b11

Bits	Name	Description	Reset
[0]	RES1	Reserved	RES1

**Access**

MRS &lt;Xt&gt;, TRCIDR0

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1000	0b111

**Accessibility**

MRS &lt;Xt&gt;, TRCIDR0

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR0;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR0;

```

**A.2.8.26 TRCEVENTCTL1R, Event Control 1 Register**

Controls the behavior of the tracing events that AArch64-TRCEVENTCTL0R selects.

**Configurations**AArch64 register TRCEVENTCTL1R bits [31:0] are architecturally mapped to External register [B.2.2.7.6 TRCEVENTCTL1R, Event Control 1 Register](#) on page 2092 bits [31:0].**Attributes****Width**

64

**Functional group**

Trace unit registers

**Access type**

See bit descriptions

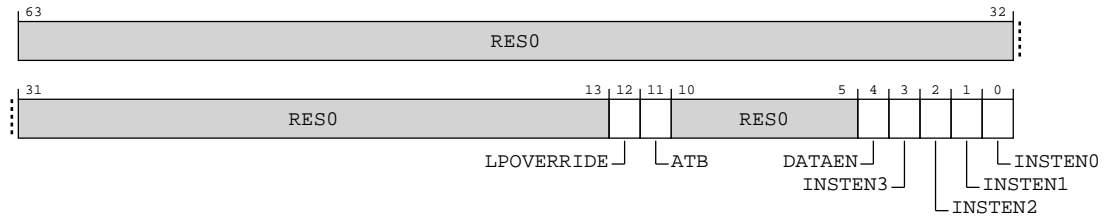
**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-410: AARCH64\_TRCEVENTCTL1R bit assignments****Table A-1049: TRCEVENTCTL1R bit descriptions**

Bits	Name	Description	Reset
[63:13]	RES0	Reserved	RES0
[12]	LPOVERRIDE	<p>Low-power Override Mode select.</p> <p><b>0b0</b></p> <p>Trace unit Low-power Override Mode is not enabled. That is, the trace unit is permitted to enter low-power state.</p> <p><b>0b1</b></p> <p>Trace unit Low-power Override Mode is enabled. That is, entry to a low-power state does not affect the trace unit resources or trace generation.</p>	x
[11]	ATB	<p>AMBA Trace Bus (ATB) trigger enable.</p> <p>When trace event 0 occurs the trace unit sets:</p> <ul style="list-style-type: none"> <li>ATID == 0x7D.</li> <li>ATDATA to the value of AArch64-TRCTRACEIDR.</li> </ul> <p>If the width of ATDATA is greater than the width of AArch64-TRCTRACEIDR.TRACEID then the trace unit zeros the upper ATDATA bits.</p> <p>If trace event 0 is programmed to occur based on program execution, such as an address comparator, the ATB trigger might not be inserted into the ATB stream at the same time as any trace generated by that program execution is output by the trace unit. Typically, the generated trace might be buffered in a trace unit which means that the ATB trigger would be output before the associated trace is output.</p> <p>If trace event 0 is asserted multiple times in close succession, the trace unit is required to generate an ATB trigger for the first assertion, but might ignore one or more of the subsequent assertions. Arm recommends that the window in which ETMEvent 0 is ignored is limited only by the time taken to output an ATB trigger.</p> <p><b>0b0</b></p> <p>ATB trigger is disabled.</p> <p><b>0b1</b></p> <p>ATB trigger is enabled.</p>	x

Bits	Name	Description	Reset
[10:5]	<b>RES0</b>	Reserved	<b>RES0</b>
[4]	DATAEN	Data event enable bit.  <b>0b0</b> If event 0 occurs, the trace unit does not generate an Event element.  <b>0b1</b> If event 0 occurs, the trace unit generates an Event element in the data trace stream.	x
[3:0]	INSTEN<m>, bit[m], where m = 3 to 0	Event element control.  <b>0b0</b> The trace unit does not generate an Event element m.  <b>0b1</b> The trace unit generates an Event element m.	xxxx

### Access

Must be programmed.

MRS <Xt>, TRCEVENTCTL1R

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1001	0b000

MSR TRCEVENTCTL1R, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1001	0b000

### Accessibility

Must be programmed.

MRS <Xt>, TRCEVENTCTL1R

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEVENTCTL1R;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCEVENTCTL1R;

```

MSR TRCEVENTCTL1R, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then

```

```
if CPACR_EL1.TTA == '1' then
    AArch64.SystemAccessTrap(EL1, 0x18);
elsif CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    TRCEVENTCTL1R = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCEVENTCTL1R = X[t, 64];
```

### A.2.8.27 TRCVDSACCTLR, ViewData Include/Exclude Single Address Comparator Control Register

Use this to select, or read, the Single Address Comparators for the ViewData include/exclude control.

#### Configurations

AArch64 register TRCVDSACCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.17 TRCVDSACCTLR, ViewData Include/Exclude Single Address Comparator Control Register](#) on page 2114 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

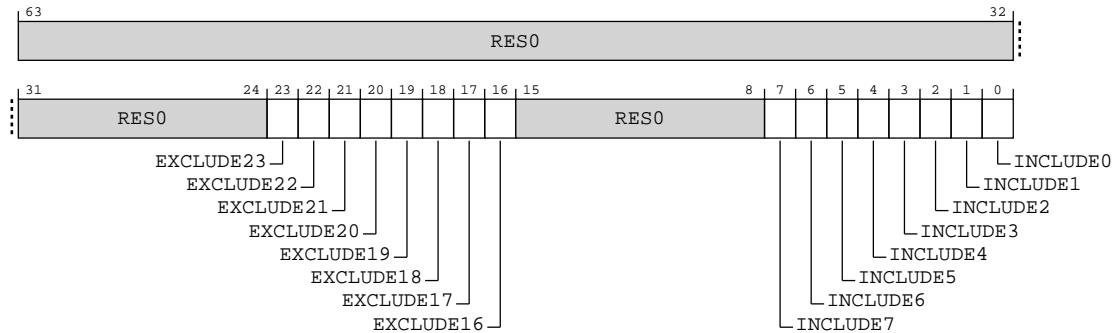


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-411: AARCH64\_TRCVDSACCTLR bit assignments**



**Table A-1052: TRCVDSACCTLR bit descriptions**

Bits	Name	Description	Reset
[63:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:16]	EXCLUDE<m>, bit[m], where $m = 23$ to 16	<p>Selects which single address comparators are in use with ViewData exclude control..</p> <p><b>0b0</b></p> <p>The single address comparator <math>m</math>, is not selected for exclude control.</p> <p><b>0b1</b></p> <p>The single address comparator <math>m</math>, is selected for exclude control.</p>	$8\{x\}$
[15:8]	<b>RES0</b>	Reserved	<b>RES0</b>
[7:0]	INCLUDE<m>, bit[m], where $m = 7$ to 0	<p>Selects which single address comparators are in use with ViewData include control.</p> <p><b>0b0</b></p> <p>The single address comparator <math>m</math>, is not selected for include control.</p> <p><b>0b1</b></p> <p>The single address comparator <math>m</math>, is selected for include control.</p> <p>If no single address comparators and no address range comparators are selected to be included, then all data transfers are included by default. The exclude control then indicates which data transfers are excluded.</p>	$8\{x\}$

## Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects a single address comparator that is either:

- Programmed to be sensitive to a data value comparator.

- Programmed to be an instruction address comparator.

In these situations, data transfers might be traced unexpectedly or might not be traced.

MRS <Xt>, TRCVDSACCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1001	0b010

MSR TRCVDSACCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1001	0b010

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects a single address comparator that is either:

- Programmed to be sensitive to a data value comparator.
- Programmed to be an instruction address comparator.

In these situations, data transfers might be traced unexpectedly or might not be traced.

MRS <Xt>, TRCVDSACCTLR

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDSACCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDSACCTLR;
```

MSR TRCVDSACCTLR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
```

```
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDSACCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDSACCTLR = X[t, 64];
```

A.2.8.28 TRCIDR1, ID Register 1

Returns the tracing capabilities of the trace unit.

Configurations

AArch64 register TRCIDR1 bits [31:0] are architecturally mapped to External register [B.2.2.7.34 TRCIDR1, ID Register 1](#) on page 2141 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

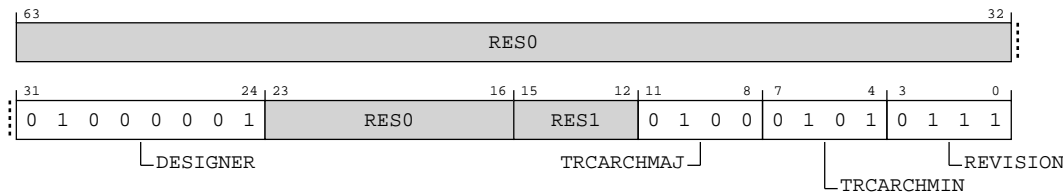
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0100	0001	xxxx	xxxx	xxxx	0100	0101	0111
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-412: AARCH64\_TRCIDR1 bit assignments





**Table A-1055: TRCIDR1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:24]	DESIGNER	Indicates which company designed the trace unit.  <b>0b01000001</b> Arm Limited.	0x41
[23:16]	RES0	Reserved	RES0
[15:12]	RES1	Reserved	RES1
[11:8]	TRCARCHMAJ	Major architecture version.  <b>0b0100</b> ETMv4.	0b0100
[7:4]	TRCARCHMIN	Minor architecture version.  <b>0b0101</b> ETMv4.5.	0b0101
[3:0]	REVISION	Implementation revision.  <b>0b0111</b> Revision 7.	0b0111

### Access

MRS &lt;Xt&gt;, TRCIDR1

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1001	0b111

### Accessibility

MRS &lt;Xt&gt;, TRCIDR1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR1;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR1;

```

A.2.8.29 TRCVDARCCTLR, ViewData Include/Exclude Address Range Comparator Control Register

Use this to select, or read, the Address Range Comparator for the ViewData include/exclude control.

Configurations

AArch64 register TRCVDARCCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.18 TRCVDARCCTLR, ViewData Include/Exclude Address Range Comparator Control Register](#) on page 2117 bits [31:0].

Attributes

Width

64

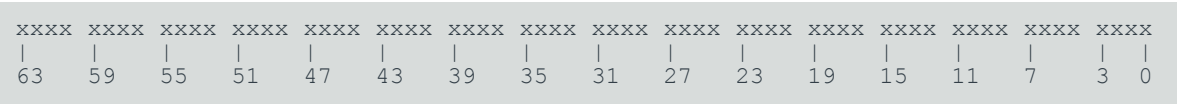
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-413: AARCH64\_TRCVDARCCTLR bit assignments

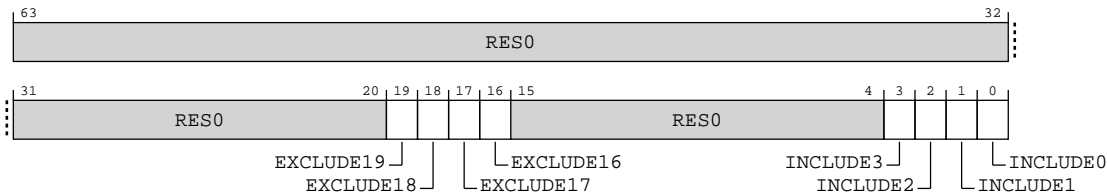


Table A-1057: TRCVDARCCTLR bit descriptions

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[19:16]	EXCLUDE<m>, bit[m], where m = 19 to 16	<p>Exclude range field. Selects which address range comparator pairs are in use with ViewData exclude control.</p> <p><b>0b0</b></p> <p>The address range that address range comparator pair m defines, is not selected for ViewData exclude control.</p> <p><b>0b1</b></p> <p>The address range that address range comparator pair m defines, is selected for ViewData exclude control.</p>	xxxx
[15:4]	RES0	Reserved	RES0
[3:0]	INCLUDE<m>, bit[m], where m = 3 to 0	<p>Include range field. Selects which address range comparator pairs are in use with ViewData include control.</p> <p><b>0b0</b></p> <p>The address range that address range comparator pair m defines, is not selected for ViewData include control.</p> <p><b>0b1</b></p> <p>The address range that address range comparator pair m defines, is selected for ViewData include control.</p> <p>If no single address comparators and no address range comparators are selected to be included, then all data transfers are included by default. The exclude control then indicates which data transfers are excluded.</p>	xxxx

## Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects an address range comparator that is programmed to be sensitive to a data value comparator, data transfers might be traced unexpectedly or might not be traced.

MRS <Xt>, TRCVDARCCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1010	0b010

MSR TRCVDARCCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1010	0b010

## Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, AArch64-TRCCONFIGR.DA==1 or AArch64-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, AArch64-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects an address range comparator that is programmed to be sensitive to a data value comparator, data transfers might be traced unexpectedly or might not be traced.

MRS <Xt>, TRCVDARCCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDARCCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVDARCCTLR;

```

MSR TRCVDARCCTLR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDARCCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVDARCCTLR = X[t, 64];

```

### A.2.8.30 TRCIDR2, ID Register 2

Returns the tracing capabilities of the trace unit.

## Configurations

AArch64 register TRCIDR2 bits [31:0] are architecturally mapped to External register [B.2.2.7.35 TRCIDR2, ID Register 2](#) on page 2143 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1100	0000	1000	0100	0001	0000	1000	1000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-414: AARCH64\_TRCIDR2 bit assignments

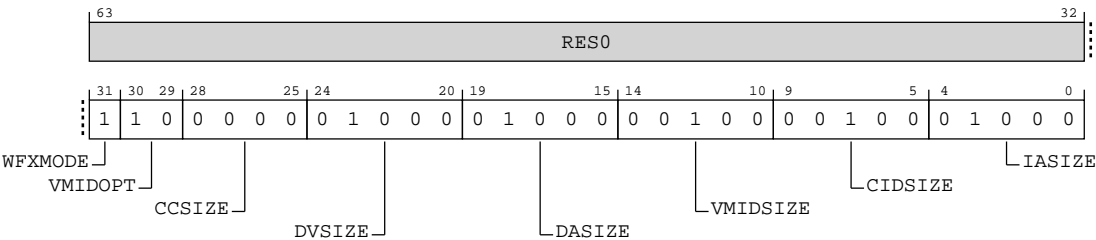


Table A-1060: TRCIDR2 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	WFXMODE	Indicates whether WFI and WFE instructions are classified as P0 instructions:  <b>0b1</b> WFI and WFE instructions are classified as P0 instructions.	0b1
[30:29]	VMIDOPT	Indicates the options for Virtual context identifier selection.  <b>0b10</b> Virtual context identifier selection not supported. AArch64-TRCCONFIGR.VMIDOPT is <b>RES1</b> .	0b10
[28:25]	CCSIZE	Indicates the size of the cycle counter.  <b>0b0000</b> The cycle counter is 12 bits in length.  All other values are reserved.	0b0000

Bits	Name	Description	Reset
[24:20]	DVSIZE	Indicates the data value size in bytes.  <b>0b01000</b> Data value tracing has a maximum of 64-bit data values.	0b01000
[19:15]	DASIZE	Indicates the data address size in bytes.  <b>0b01000</b> Data address tracing has a maximum of 64-bit data addresses.	0b01000
[14:10]	VMIDSIZE	Indicates the trace unit Virtual context identifier size.  <b>0b00100</b> 32-bit Virtual context identifier size.	0b00100
[9:5]	CIDSIZE	Indicates the Context identifier size.  <b>0b00100</b> 32-bit Context identifier size.	0b00100
[4:0]	IASIZE	Virtual instruction address size.  <b>0b01000</b> Maximum of 64-bit instruction address size.	0b01000

## Access

MRS <Xt>, TRCIDR2

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1010	0b111

## Accessibility

MRS <Xt>, TRCIDR2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR2;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR2;

```

### A.2.8.31 TRCSTALLCTLR, Stall Control Register

Enables trace unit functionality that prevents trace unit buffer overflows.

## Configurations

AArch64 register TRCSTALLCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.7 TRCSTALLCTLR, Stall Control Register](#) on page 2094 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-415: AARCH64\_TRCSTALLCTLR bit assignments

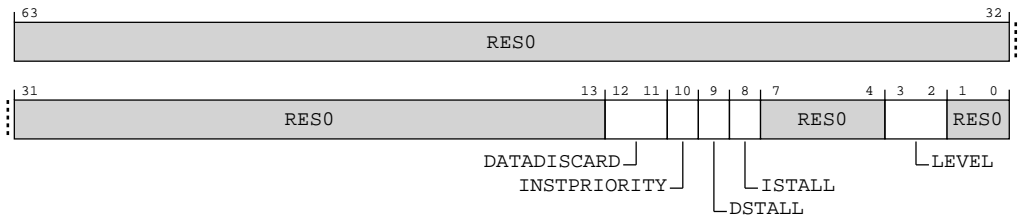


Table A-1062: TRCSTALLCTLR bit descriptions

Bits	Name	Description	Reset
[63:13]	RES0	Reserved	RES0
[12:11]	DATADISCARD	Data discard field. Controls if a trace unit can discard data trace elements when the data trace buffer space is less than LEVEL.  <b>0b00</b> The trace unit must not discard any data trace elements.  <b>0b01</b> The trace unit can discard P1 and P2 elements associated with data loads.  <b>0b10</b> The trace unit can discard P1 and P2 elements associated with data stores.  <b>0b11</b> The trace unit can discard P1 and P2 elements associated with both data loads and stores.	xx

Bits	Name	Description	Reset
[10]	INSTPRIORITY	<p>Prioritize instruction trace bit. Controls if a trace unit can prioritize instruction trace when the instruction trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not prioritize instruction trace.</p> <p><b>0b1</b> The trace unit can prioritize instruction trace. A trace unit might prioritize</p>	x
[9]	DSTALL	<p>Data stall bit. Controls if a trace unit can stall the PE when the data trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not stall the PE.</p> <p><b>0b1</b> The trace unit can stall the PE.</p>	x
[8]	ISTALL	<p>Instruction stall control. Controls if a trace unit can stall the PE when the trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not stall the PE.</p> <p><b>0b1</b> The trace unit can stall the PE.</p>	x
[7:4]	RES0	Reserved	RES0
[3:2]	LEVEL	<p>Threshold level field. The field supports 4 monotonic levels from 0b00 to 0b11.</p> <p><b>0b00</b> Minimal invasion. This setting has a greater risk of a trace unit buffer overflow.</p> <p><b>0b01</b> Small invasion.</p> <p><b>0b10</b> Big invasion.</p> <p><b>0b11</b> Maximum invasion. Reduced risk of a trace unit buffer overflow.</p>	xx
[1:0]	RES0	Reserved	RES0

## Access

Must be programmed if implemented.

MRS <Xt>, TRCSTALLCTL

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1011	0b000

MSR TRCSTALLCTL, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1011	0b000



## Accessibility

Must be programmed if implemented.

MRS <Xt>, TRCSTALLCTL

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSTALLCTL;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSTALLCTL;

```

MSR TRCSTALLCTL, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSTALLCTL = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSTALLCTL = X[t, 64];

```

### A.2.8.32 TRCIDR3, ID Register 3

Returns the base architecture of the trace unit.

#### Configurations

AArch64 register TRCIDR3 bits [31:0] are architecturally mapped to External register [B.2.2.7.36 TRCIDR3, ID Register 3](#) on page 2145 bits [31:0].

#### Attributes

##### Width

64

##### Functional group

Trace unit registers

##### Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000	1101	x000	0111	xx00	0000	0000	0100
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-416: AARCH64\_TRCIDR3 bit assignments

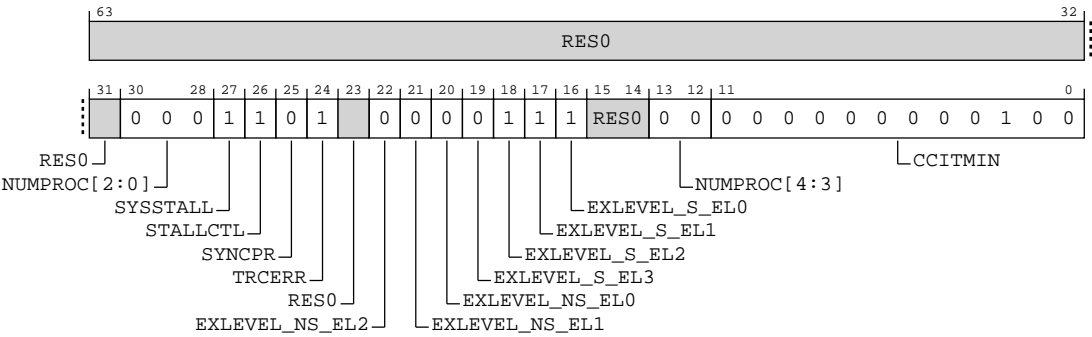


Table A-1065: TRCIDR3 bit descriptions

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0
[27]	SYSSTALL	Indicates if stalling of the PE is permitted.  0b1 Stalling of the PE is permitted.	0b1
[26]	STALLCTL	Indicates if trace unit implements stalling of the PE.  0b1 Stalling of the PE is implemented.	0b1
[25]	SYNCPR	Indicates if an implementation has a fixed synchronization period.  0b0 AArch64-TRCSYNCPR is read-write so software can change the synchronization period.	0b0
[24]	TRCERR	Indicates forced tracing of System Error exceptions is implemented.  0b1 Forced tracing of System Error exceptions is implemented.	0b1
[23]	RES0	Reserved	RES0
[22]	EXLEVEL_NS_EL2	Indicates if Non-secure EL2 implemented.  0b0 Non-secure EL2 is not implemented.	0b0

Bits	Name	Description	Reset
[21]	EXLEVEL_NS_EL1	Indicates if Non-secure EL1 implemented.  <b>0b0</b> Non-secure EL1 is not implemented.	0b0
[20]	EXLEVEL_NS_ELO	Indicates if Non-secure ELO implemented.  <b>0b0</b> Non-secure ELO is not implemented.	0b0
[19]	EXLEVEL_S_EL3	Indicates if Secure EL3 implemented.  <b>0b0</b> Secure EL3 is not implemented.	0b0
[18]	EXLEVEL_S_EL2	Indicates if Secure EL2 implemented.  <b>0b1</b> Secure EL2 is implemented.	0b1
[17]	EXLEVEL_S_EL1	Indicates if Secure EL1 implemented.  <b>0b1</b> Secure EL1 is implemented.	0b1
[16]	EXLEVEL_S_ELO	Indicates if Secure ELO implemented.  <b>0b1</b> Secure ELO is implemented.	0b1
[15:14]	<b>RES0</b>	Reserved	<b>RES0</b>
[13:12, 30:28]	NUMPROC	Indicates the number of PEs available for tracing.  <b>0b000000</b> The trace unit can trace one PE.  This field reads as 0b000000.	0b000000
[11:0]	CCITMIN	Indicates the minimum value that can be programmed in AArch64-TRCCCCTLR.THRESHOLD.  <b>0b0000000000100</b> Minimum allowed threshold value is 4.	0x004

## Access

MRS <Xt>, TRCIDR3

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1011	0b111

## Accessibility

MRS <Xt>, TRCIDR3

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else

```

```
        X[t, 64] = TRCIDR3;
    elseif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCIDR3;
```

A.2.8.33 TRCTSCTLR, Timestamp Control Register

Controls the insertion of global timestamps in the trace stream.

Configurations

AArch64 register TRCTSCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.8 TRCTSCTLR, Timestamp Control Register](#) on page 2097 bits [31:0].

Attributes

Width

64

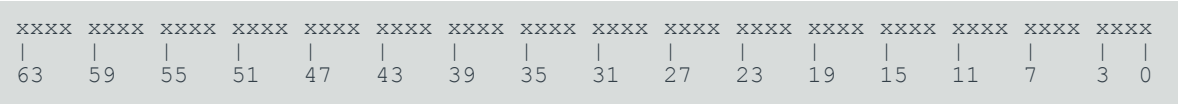
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-417: AARCH64\_TRCTSCTLR bit assignments

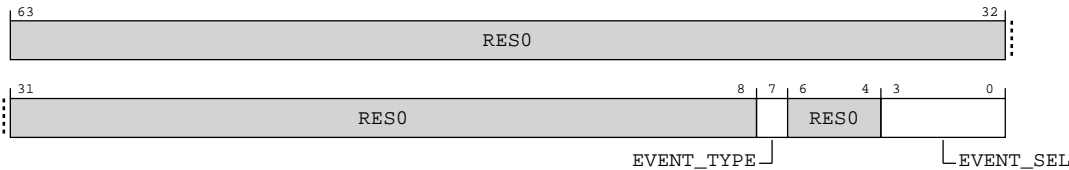


Table A-1067: TRCTSCTLR bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7]	EVENT_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

## Access

Must be programmed if AArch64-TRCCONFIGR.TS == 0b1.

MRS <Xt>, TRCTSCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1100	0b000

MSR TRCTSCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1100	0b000

## Accessibility

Must be programmed if AArch64-TRCCONFIGR.TS == 0b1.

MRS <Xt>, TRCTSCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCTSCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCTSCTLR;

```

MSR TRCTSCTLR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCTSCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCTSCTLR = X[t, 64];
```

A.2.8.34 TRCIDR4, ID Register 4

Returns the tracing capabilities of the trace unit.

Configurations

AArch64 register TRCIDR4 bits [31:0] are architecturally mapped to External register [B.2.2.7.37 TRCIDR4, ID Register 4](#) on page 2147 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0001	0010	0111	0000	xxx1	0010	0100
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure A-418: AARCH64\_TRCIDR4 bit assignments

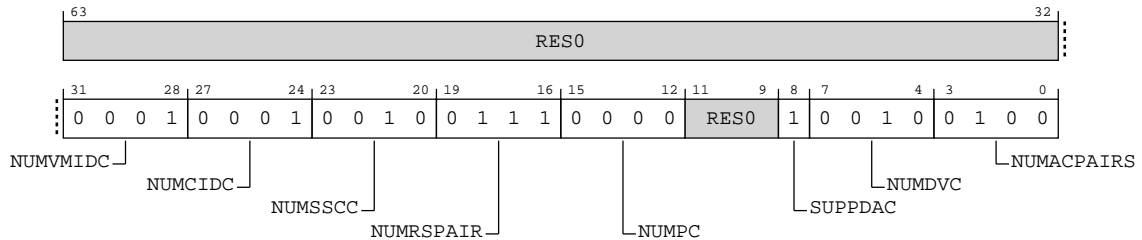


Table A-1070: TRCIDR4 bit descriptions

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:28]	NUMVMIDC	Indicates the number of Virtual Context Identifier Comparators that are available for tracing. <b>0b0001</b> The implementation has one Virtual Context Identifier Comparator.	0b0001
[27:24]	NUMCIDC	Indicates the number of Context Identifier Comparators that are available for tracing. <b>0b0001</b> The implementation has one Context Identifier Comparator.	0b0001
[23:20]	NUMSSCC	Indicates the number of Single-shot Comparator Controls that are available for tracing. <b>0b0010</b> The implementation has two Single-shot Comparator Controls.	0b0010
[19:16]	NUMRSPAIR	Indicates the number of resource selector pairs that are available for tracing. <b>0b0111</b> The implementation has eight resource selector pairs.	0b0111
[15:12]	NUMPC	Indicates the number of PE Comparator Inputs that are available for tracing. <b>0b0000</b> No PE Comparator Inputs are available.	0b0000
[11:9]	<b>RES0</b>	Reserved	<b>RES0</b>
[8]	SUPPDAC	Indicates whether data address comparisons are implemented. <b>0b1</b> Data address comparisons implemented.	0b1
[7:4]	NUMDVC	Indicates the number of data value comparators. <b>0b0010</b> Two data value comparators implemented.	0b0010
[3:0]	NUMACPAIRS	Indicates the number of address comparator pairs that are available for tracing. <b>0b0100</b> The implementation has four address comparator pairs.	0b0100

## Access

MRS &lt;Xt&gt;, TRCIDR4

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1100	0b111

Accessibility

MRS <Xt>, TRCIDR4

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR4;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR4;
```

A.2.8.35 TRCSYNCP, Synchronization Period Register

Controls how often trace protocol synchronization requests occur.

Configurations

AArch64 register TRCSYNCP bits [31:0] are architecturally mapped to External register [B.2.2.7.9 TRCSYNCP, Synchronization Period Register](#) on page 2098 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-419: AARCH64\_TRCSYNCPR bit assignments

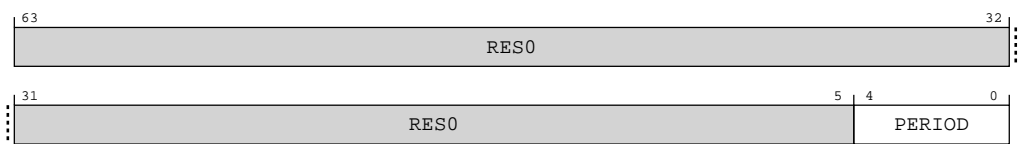


Table A-1072: TRCSYNCPR bit descriptions

Bits	Name	Description	Reset
[63:5]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[4:0]	PERIOD	<p>Defines the number of bytes of trace between each periodic trace protocol synchronization request.</p> <p><b>0b000000</b> Trace protocol synchronization is disabled.</p> <p><b>0b010000</b> Trace protocol synchronization request occurs after <math>2^8</math> bytes of trace.</p> <p><b>0b01001</b> Trace protocol synchronization request occurs after <math>2^9</math> bytes of trace.</p> <p><b>0b01010</b> Trace protocol synchronization request occurs after <math>2^{10}</math> bytes of trace.</p> <p><b>0b01011</b> Trace protocol synchronization request occurs after <math>2^{11}</math> bytes of trace.</p> <p><b>0b01100</b> Trace protocol synchronization request occurs after <math>2^{12}</math> bytes of trace.</p> <p><b>0b01101</b> Trace protocol synchronization request occurs after <math>2^{13}</math> bytes of trace.</p> <p><b>0b01110</b> Trace protocol synchronization request occurs after <math>2^{14}</math> bytes of trace.</p> <p><b>0b01111</b> Trace protocol synchronization request occurs after <math>2^{15}</math> bytes of trace.</p> <p><b>0b10000</b> Trace protocol synchronization request occurs after <math>2^{16}</math> bytes of trace.</p> <p><b>0b10001</b> Trace protocol synchronization request occurs after <math>2^{17}</math> bytes of trace.</p> <p><b>0b10010</b> Trace protocol synchronization request occurs after <math>2^{18}</math> bytes of trace.</p> <p><b>0b10011</b> Trace protocol synchronization request occurs after <math>2^{19}</math> bytes of trace.</p> <p><b>0b10100</b> Trace protocol synchronization request occurs after <math>2^{20}</math> bytes of trace.</p> <p>Other values are reserved. If a reserved value is programmed into PERIOD, then one of the following behaviors occurs:</p> <ul style="list-style-type: none"> <li>If a reserved value less than 0b010000 is programmed, trace protocol synchronisation requests occur at approximately the specified period.</li> <li>If a reserved value greater than 0b101000 is programmed, no trace protocol synchronisation requests are generated.</li> </ul>	5 {x}

## Access

Must be programmed if AArch64-TRCIDR3.SYNCPR == 0b0.

MRS <Xt>, TRCSYNCPR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1101	0b000

MSR TRCSYNCPR, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1101	0b000

**Accessibility**

Must be programmed if AArch64-TRCIDR3.SYNCPR == 0b0.

MRS &lt;Xt&gt;, TRCSYNCPR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSYNCPR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSYNCPR;

```

MSR TRCSYNCPR, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSYNCPR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSYNCPR = X[t, 64];

```

**A.2.8.36 TRCIDR5, ID Register 5**

Returns the tracing capabilities of the trace unit.

**Configurations**AArch64 register TRCIDR5 bits [31:0] are architecturally mapped to External register [B.2.2.7.38 TRCIDR5, ID Register 5](#) on page 2149 bits [31:0].**Attributes****Width**

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0010	100x	1100	0111	xxxx	1000	0011	1010
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-420: AARCH64\_TRCIDR5 bit assignments

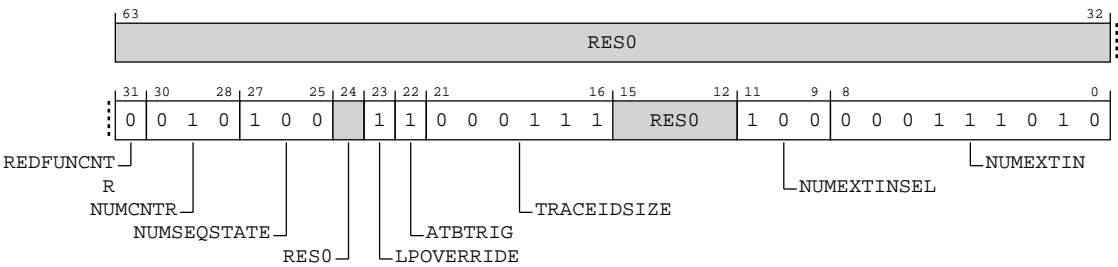


Table A-1075: TRCIDR5 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	REDFUNCNTR	Indicates if the reduced function counter is implemented. <b>0b0</b> The reduced function counter is not supported.	0b0
[30:28]	NUMCNTR	Indicates the number of counters that are available for tracing. <b>0b010</b> Two counters implemented.	0b010
[27:25]	NUMSEQSTATE	Indicates if the sequencer is implemented and the number of sequencer states that are implemented. <b>0b100</b> Four sequencer states are implemented.	0b100
[24]	RES0	Reserved	RES0
[23]	LPOVERRIDE	Indicates support for Low-power Override Mode. <b>0b1</b> The trace unit support Low-power Override Mode.	0b1

Bits	Name	Description	Reset
[22]	ATBTRIG	Indicates if the implementation can support ATB triggers. <b>0b1</b> The implementation supports ATB triggers.	0b1
[21:16]	TRACEIDSIZE	Indicates the trace ID width. <b>0b000111</b> The implementation supports a 7-bit trace ID.	0b000111
[15:12]	RES0	Reserved	RES0
[11:9]	NUMEXTINSEL	Indicates how many external input selector resources are implemented. <b>0b100</b> 4 external input selector resources are available.	0b100
[8:0]	NUMEXTIN	Indicates how many external inputs are implemented. <b>0b000111010</b> The implementation has 58 external inputs.	0b000111010

### Access

MRS <Xt>, TRCIDR5

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1101	0b111

### Accessibility

MRS <Xt>, TRCIDR5

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR5;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR5;

```

## A.2.8.37 TRCCCCTLR, Cycle Count Control Register

Set the threshold value for cycle counting.

### Configurations

AArch64 register TRCCCCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.10 TRCCCCTLR, Cycle Count Control Register](#) on page 2101 bits [31:0].

Attributes

Width

64

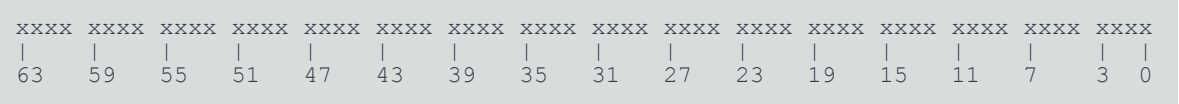
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-421: AARCH64\_TRCCCCTLR bit assignments

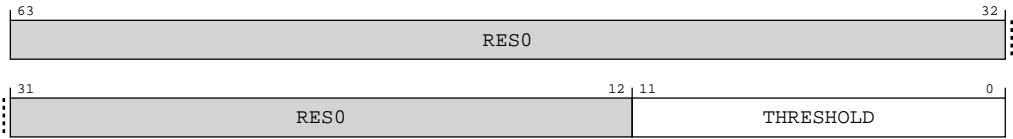


Table A-1077: TRCCCCTLR bit descriptions

Bits	Name	Description	Reset
[63:12]	RES0	Reserved	RES0
[11:0]	THRESHOLD	<div>Sets the threshold value for instruction trace cycle counting.</div> <div>The minimum threshold value that can be programmed into THRESHOLD is given in AArch64-TRCIDR3.CCITMIN. If the THRESHOLD value is smaller than the value in AArch64-TRCIDR3.CCITMIN, then no cycle counts are generated in the trace and the cycle count threshold is not included in a traceinfo packet.</div> <div>Writing a value of zero when AArch64-TRCCONFIGR.CCI is set to enable instruction trace cycle counting, then no cycle counts are generated in the trace and the cycle count threshold is not included in a traceinfo packet.</div>	12 {x}

Access

Must be programmed if AArch64-TRCCONFIGR.CCI == 0b1.

MRS <Xt>, TRCCCCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1110	0b000

MSR TRCCCCTLR, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1110	0b000

### Accessibility

Must be programmed if AArch64-TRCCONFIGR.CCI == 0b1.

MRS &lt;Xt&gt;, TRCCCCTLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCCCTLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCCCTLR;

```

MSR TRCCCCTLR, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCCCTLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCCCTLR = X[t, 64];

```

### A.2.8.38 TRCIDR6, ID Register 6

Returns the tracing capabilities of the trace unit.

### Configurations

AArch64 register TRCIDR6 bits [31:0] are architecturally mapped to External register [B.2.2.7.39 TRCIDR6, ID Register 6](#) on page 2150 bits [31:0].

Attributes

Width

64

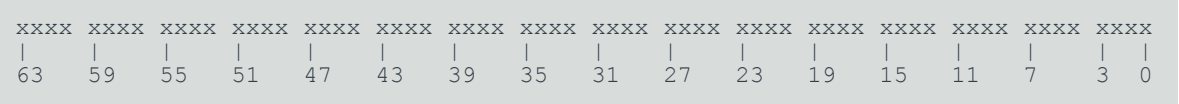
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-422: AARCH64\_TRCIDR6 bit assignments

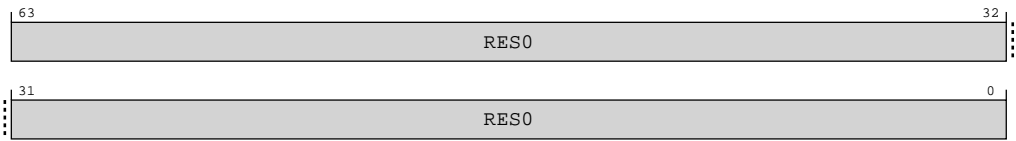


Table A-1080: TRCIDR6 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, TRCIDR6

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1110	0b111

Accessibility

MRS <Xt>, TRCIDR6

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
```



```
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR6;
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCIDR6;
```

A.2.8.39 TRCBBCTLR, Branch Broadcast Control Register

Controls the regions in the memory map where branch broadcasting is active.

Configurations

AArch64 register TRCBBCTLR bits [31:0] are architecturally mapped to External register [B.2.2.7.11 TRCBBCTLR, Branch Broadcast Control Register](#) on page 2102 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

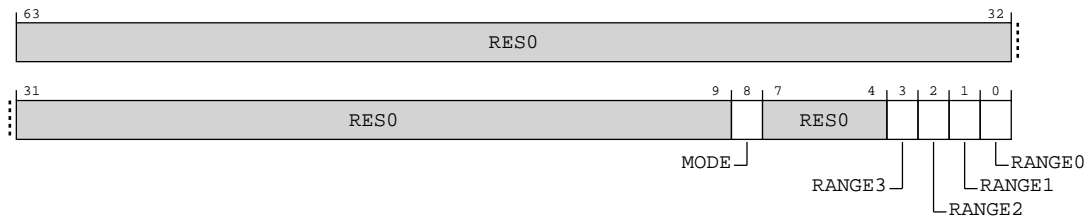


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-423: AARCH64\_TRCBBCTLR bit assignments



**Table A-1082: TRCBBCTLR bit descriptions**

Bits	Name	Description	Reset
[63:9]	RES0	Reserved	RES0
[8]	MODE	<p>Mode.</p> <p><b>0b0</b></p> <p>Exclude Mode.</p> <p>Branch broadcasting is not active for instructions in the address ranges defined by RANGE.</p> <p>If RANGE == 0x00 then branch broadcasting is active for all instructions.</p> <p><b>0b1</b></p> <p>Include Mode.</p> <p>Branch broadcasting is active for instructions in the address ranges defined by RANGE.</p> <p>If RANGE == 0x00 then no instructions are considered to be in the branch broadcasting region.</p>	x
[7:4]	RES0	Reserved	RES0
[3:0]	RANGE<m>, bit[m], where m = 3 to 0	<p>Address range field.</p> <p>Selects which Address Range Comparators are in use with branch broadcasting.</p> <p><b>0b0</b></p> <p>The address range that Address Range Comparator m defines, is not selected.</p> <p><b>0b1</b></p> <p>The address range that Address Range Comparator m defines, is selected.</p>	xxxx

### Access

Must be programmed if AArch64-TRCCONFIGR.BB == 0b1.

MRS <Xt>, TRCBBCTLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1111	0b000

MSR TRCBBCTLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1111	0b000

### Accessibility

Must be programmed if AArch64-TRCCONFIGR.BB == 0b1.

MRS <Xt>, TRCBBCTLR

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
```

```

    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCBBCTLR;
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCBBCTLR;

```

MSR TRCBBCTLR, &lt;Xt&gt;

```

    if PSTATE.EL == EL0 then
        UNDEFINED;
    elsif PSTATE.EL == EL1 then
        if CPACR_EL1.TTA == '1' then
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            TRCBBCTLR = X[t, 64];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            TRCBBCTLR = X[t, 64];

```

#### A.2.8.40 TRCIDR7, ID Register 7

Returns the tracing capabilities of the trace unit.

##### Configurations

AArch64 register TRCIDR7 bits [31:0] are architecturally mapped to External register [B.2.2.7.40 TRCIDR7, ID Register 7](#) on page 2152 bits [31:0].

##### Attributes

###### Width

64

###### Functional group

Trace unit registers

###### Access type

See bit descriptions

###### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-424: AARCH64\_TRCIDR7 bit assignments

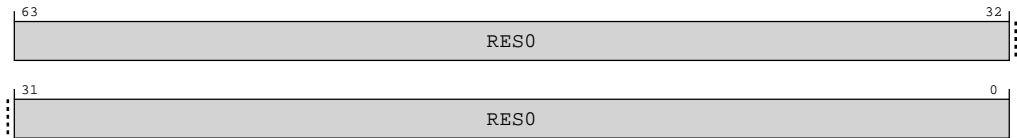


Table A-1085: TRCIDR7 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, TRCIDR7

op0	op1	CRn	CRm	op2
0b10	0b001	0b0000	0b1111	0b111

Accessibility

MRS <Xt>, TRCIDR7

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR7;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCIDR7;
```

A.2.8.41 TRCSSCCR<n>, Single-shot Comparator Control Register <n> , n = 0 - 1

Controls the corresponding Single-shot Comparator Control resource.

Configurations

AArch64 register TRCSSCCR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.42 TRCSSCCR<n>, Single-shot Comparator Control Register <n> , n = 0 - 1](#) on page 2159 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-425: AARCH64\_TRCSSCCR<n> bit assignments

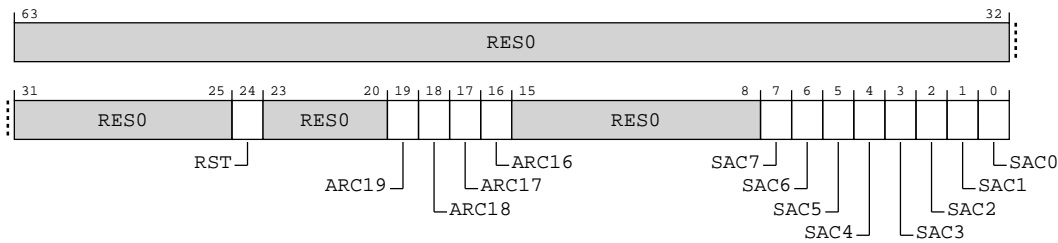


Table A-1087: TRCSSCCR<n> bit descriptions

Bits	Name	Description	Reset
[63:25]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[24]	RST	Selects the Single-shot Comparator Control mode.  <b>0b0</b> The Single-shot Comparator Control is in single-shot mode.  <b>0b1</b> The Single-shot Comparator Control is in multi-shot mode.	x
[23:20]	RES0	Reserved	RES0
[19:16]	ARC<m>, bit[m], where m = 19 to 16	Selects one or more Address Range Comparators for Single-shot control.  <b>0b0</b> The Address Range Comparator m, is not selected for Single-shot control.  <b>0b1</b> The Address Range Comparator m, is selected for Single-shot control.	xxxx
[15:8]	RES0	Reserved	RES0
[7:0]	SAC<m>, bit[m], where m = 7 to 0	Selects one or more Single Address Comparators for Single-shot control.  <b>0b0</b> The Single Address Comparator m, is not selected for Single-shot control.  <b>0b1</b> The Single Address Comparator m, is selected for Single-shot control.	8{x}

## Access

Must be programmed if any TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

MRS <Xt>, TRCSSCCR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	'0':m[2:0]	0b010

MSR TRCSSCCR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	'0':m[2:0]	0b010

## Accessibility

Must be programmed if any TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

MRS <Xt>, TRCSSCCR<m>

```
integer m = UInt(CRm<2:0>);
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

```
        X[t, 64] = TRCSSCCR[m];
    elseif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCSSCCR[m];
```

MSR TRCSSCCR<m>, <Xt>

```
integer m = UInt(CRm<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSSCCR[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSSCCR[m] = X[t, 64];
```

A.2.8.42 TRCSSCSR<n>, Single-shot Comparator Control Status Register <n> , n = 0 - 1

Returns the status of the corresponding Single-shot Comparator Control.

Configurations

AArch64 register TRCSSCSR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.43 TRCSSCSR<n>, Single-shot Comparator Control Status Register <n> , n = 0 - 1](#) on page 2161 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

RO

Reset value

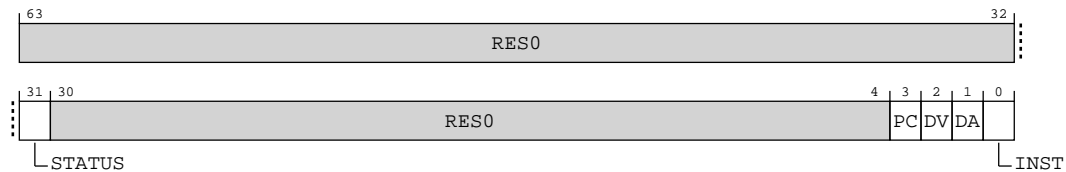
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-426: AARCH64\_TRCSSCSR<n> bit assignments**



**Table A-1090: TRCSSCSR<n> bit descriptions**

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	STATUS	<p>Single-shot Comparator Control status. Indicates if any of the comparators selected by this Single-shot Comparator control have matched. The selected comparators are defined by AArch64-TRCSSCCR&lt;n&gt;.ARC and AArch64-TRCSSCCR&lt;n&gt;.SAC.</p> <p><b>0b0</b></p> <p>No match has occurred. When the first match occurs, this field takes a value of 0b1. It remains at 0b1 until explicitly modified by a write to this register.</p> <p><b>0b1</b></p> <p>One or more matches has occurred. If AArch64-TRCSSCCR&lt;n&gt;.RST == 0b0 then:</p> <ul style="list-style-type: none"> <li>There is only one match and no more matches are possible.</li> <li>Software must reset this bit to 0b0 to re-enable the Single-shot Comparator Control.</li> </ul> <p>The reset value is <b>UNKNOWN</b>. STATUS must be written to set an initial state when programming the trace unit, if the single-shot comparator is to be used.</p>	x
[30:4]	RES0	Reserved	RES0
[3]	PC	<p>PE Comparator Input support.</p> <p><b>0b0</b></p> <p>This Single-shot Comparator Control does not support PE Comparator Inputs.</p>	x
[2]	DV	<p>Data value comparator support.</p> <p><b>0b0</b></p> <p>This Single-shot Comparator Control does not support data value comparisons. TRCSSCSR0 has this value.</p> <p><b>0b1</b></p> <p>This Single-shot Comparator Control supports data value comparisons. TRCSSCSR1 has this value.</p>	x



Bits	Name	Description	Reset
[1]	DA	Data address comparator support.  <b>0b0</b> This Single-shot Comparator Control does not support data address comparisons. TRCSSCSR0 has this value.  <b>0b1</b> This Single-shot Comparator Control supports data address comparisons. TRCSSCSR1 has this value.	x
[0]	INST	Instruction address comparator support.  <b>0b0</b> This Single-shot Comparator Control does not support instruction address comparisons. TRCSSCSR1 has this value.  <b>0b1</b> This Single-shot Comparator Control supports instruction address comparisons. TRCSSCSR0 has this value.	x

### Access

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

MRS <Xt>, TRCSSCSR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	'1':m[2:0]	0b010

MSR TRCSSCSR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	'1':m[2:0]	0b010

### Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

MRS <Xt>, TRCSSCSR<m>

```

integer m = UInt(CRm<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSSCSR[m];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCSSCSR[m];

```

MSR TRCSSCSR<m>, <Xt>

```
integer m = UInt(CRm<2:0>);
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSSCSR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCSSCSR[m] = X[t, 64];
```

A.2.8.43 TRCOSLAR, Trace OS Lock Access Register

Controls whether the Trace OS Lock is locked.

Configurations

AArch64 register TRCOSLAR bits [31:0] are architecturally mapped to External register [B.2.2.7.44 TRCOSLAR, Trace OS Lock Access Register](#) on page 2163 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-427: AARCH64\_TRCOSLAR bit assignments

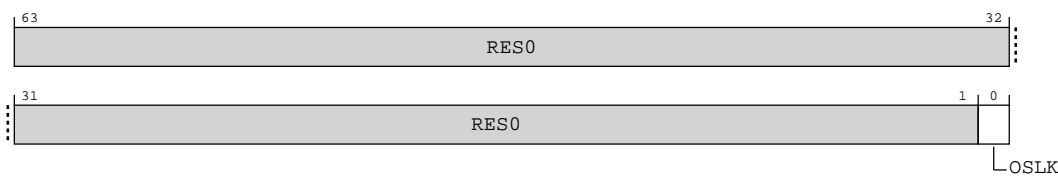


Table A-1093: TRCOSLAR bit descriptions

Bits	Name	Description	Reset
[63:1]	RES0	Reserved	RES0
[0]	OSLK	OS Lock control bit.  <b>0b0</b> Unlocks the OS Lock.  <b>0b1</b> Locks the OS Lock. This setting disables the trace unit.	x

Access

MSR TRCOSLAR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	0b0000	0b100

Accessibility

MSR TRCOSLAR, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCOSLAR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCOSLAR = X[t, 64];
```

A.2.8.44 TRCOSLSR, Trace OS Lock Status Register

Returns the status of the Trace OS Lock.

Configurations

AArch64 register TRCOSLSR bits [31:0] are architecturally mapped to External register [B.2.2.7.45 TRCOSLSR, Trace OS Lock Status Register](#) on page 2164 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1x10
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-428: AARCH64\_TRCOSLSR bit assignments

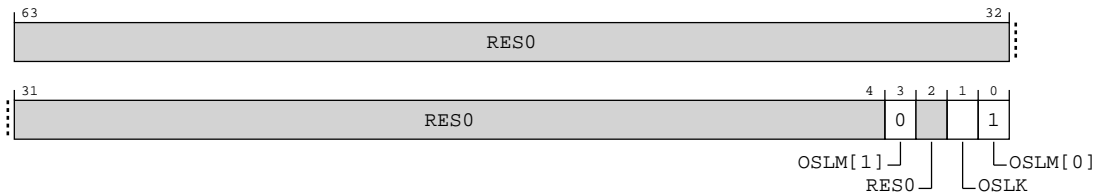


Table A-1095: TRCOSLSR bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3, 0]	OSLM	OS Lock model. <b>0b10</b> Trace OS Lock is implemented. Access to this field is: RO	0b10

Bits	Name	Description	Reset
[2]	RES0	Reserved	RES0
[1]	OSLK	OS Lock status.  <b>0b0</b> The OS Lock is unlocked.  <b>0b1</b> The OS Lock is locked.	0b1

### Access

MRS <Xt>, TRCOSLSR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	0b0001	0b100

### Accessibility

MRS <Xt>, TRCOSLSR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCOSLSR;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCOSLSR;

```

## A.2.8.45 TRCRSCTLR<n>, Resource Selection Control Register <n> , n = 2 - 15

Controls the selection of the resources in the trace unit.

### Configurations

Resource selector 0 always returns FALSE.

Resource selector 1 always returns TRUE.

Resource selectors are implemented in pairs. Each odd numbered resource selector is part of a pair with the even numbered resource selector that is numbered as one less than it. For example, resource selectors 2 and 3 form a pair.

AArch64 register TRCRSCTLR<n> bits [31:0] are architecturally mapped to External register [B.2.2.7.41 TRCRSCTLR<n>, Resource Selection Control Register <n> , n = 2 - 15](#) on page 2153 bits [31:0].

Attributes

Width

64

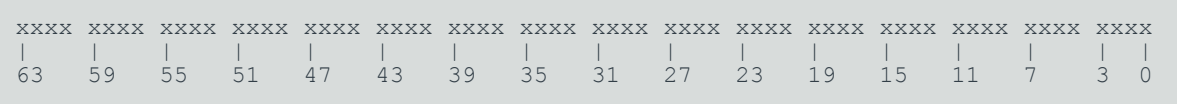
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-429: AARCH64\_TRCRSCTLR<n> bit assignments

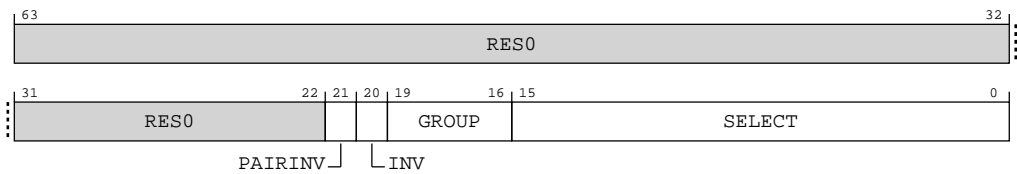


Table A-1097: TRCRSCTLR<n> bit descriptions

Bits	Name	Description	Reset
[63:22]	RES0	Reserved	RES0
[21]	PAIRINV	For TRCRSCTLR<n>, where n is even, controls whether the combined result from a resource selector pair is inverted.  <b>0b0</b> Do not invert the combined output of the 2 resource selectors.  <b>0b1</b> Invert the combined output of the 2 resource selectors.	x

Bits	Name	Description	Reset
[20]	INV	<p>Controls whether the resource, that GROUP and SELECT selects, is inverted.</p> <p><b>0b0</b> Do not invert the output of this selector.</p> <p><b>0b1</b> Invert the output of this selector.</p> <p>If:</p> <ul style="list-style-type: none"> <li>A is the register TRCRSCTLR&lt;m&gt; where m is even.</li> <li>B is the register TRCRSCTLR&lt;m+1&gt;.</li> </ul> <p>Then the combined output of the 2 resource selectors A and B depends on the value of (A.PAIRINV, A.INV, B.INV) as follows:</p> <ul style="list-style-type: none"> <li>0b000 -&gt; A and B.</li> <li>0b001 -&gt; RESERVED.</li> <li>0b010 -&gt; not(A) and B.</li> <li>0b011 -&gt; not(A) and not(B).</li> <li>0b100 -&gt; not(A) or not(B).</li> <li>0b101 -&gt; not(A) or B.</li> <li>0b110 -&gt; RESERVED.</li> <li>0b111 -&gt; A or B.</li> </ul>	x
[19:16]	GROUP	<p>Selects a group of resources.</p> <p><b>0b0000</b> External input selectors.</p> <p><b>0b0001</b> PE Comparator Inputs.</p> <p><b>0b0010</b> Counters and Sequencer.</p> <p><b>0b0011</b> Single-shot Comparator Controls.</p> <p><b>0b0100</b> Single Address Comparators.</p> <p><b>0b0101</b> Address Range Comparators.</p> <p><b>0b0110</b> Context Identifier Comparators.</p> <p><b>0b0111</b> Virtual Context Identifier Comparators.</p> <p>All other values are reserved.</p>	xxxx

Bits	Name	Description	Reset
[15:0]	SELECT	<b>SELECT encoding for External input selectors</b>  <b>15:4</b> Reserved, RES0.  <b>EXTIN&lt;m&gt;, bit[m], for m = 3 to 0</b> Selects one or more External inputs.  <b>0b0</b> Ignore EXTIN m.  <b>0b1</b> Select EXTIN m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for PE Comparator Inputs</b>  <b>15:0</b> Reserved, RES0.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Counters and Sequencer</b>  <b>15:8</b> Reserved, RES0.  <b>SEQUENCER&lt;m&gt;, bit[m], for m = 7 to 4</b> Sequencer states.  <b>0b0</b> Ignore Sequencer state m.  <b>0b1</b> Select Sequencer state m.  <b>3:2</b> Reserved, RES0.	16 {x}
[15:0 continued]	SELECT	<b>COUNTERS&lt;m&gt;, bit[m], for m = 1 to 0</b> Counters resources at zero.  <b>0b0</b> Ignore Counter m.  <b>0b1</b> Select Counter m is zero.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Single-shot Comparator Controls</b>  <b>15:2</b> Reserved, RES0.  <b>SINGLE_SHOT&lt;m&gt;, bit[m], for m = 1 to 0</b> Selects one or more Single-shot Comparator Controls.  <b>0b0</b> Ignore Single-shot Comparator Control m.  <b>0b1</b> Select Single-shot Comparator Control m.	16 {x}



Bits	Name	Description	Reset
[15:0 continued]	SELECT	<b>SELECT encoding for Single Address Comparators</b> <b>15:8</b> Reserved, RES0. <b>SAC&lt;m&gt;, bit[m], for m = 7 to 0</b> Selects one or more Single Address Comparators. <b>0b0</b> Ignore Single Address Comparator m. <b>0b1</b> Select Single Address Comparator m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Address Range Comparators</b> <b>15:4</b> Reserved, RES0. <b>ARC&lt;m&gt;, bit[m], for m = 3 to 0</b> Selects one or more Address Range Comparators. <b>0b0</b> Ignore Address Range Comparator m. <b>0b1</b> Select Address Range Comparator m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Context Identifier Comparators</b> <b>15:1</b> Reserved, RES0. <b>CID&lt;m&gt;, bit[m], for m = 0</b> Selects one or more Context Identifier Comparators. <b>0b0</b> Ignore Context Identifier Comparator m. <b>0b1</b> Select Context Identifier Comparator m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Virtual Context Identifier Comparators</b> <b>15:1</b> Reserved, RES0. <b>VMID&lt;m&gt;, bit[m], for m = 0</b> Selects one or more Virtual Context Identifier Comparators. <b>0b0</b> Ignore Virtual Context Identifier Comparator m. <b>0b1</b> Select Virtual Context Identifier Comparator m.	16 {x}

## Access

Must be programmed if any of the following are true:

- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.RLDEVENT.SEL == n.

- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.RLDEVENT.SEL == n/2.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.CNTEVENT.SEL == n.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.CNTEVENT.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT0.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT0.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT0.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT0.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT1.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT1.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT1.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT1.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT2.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT2.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT2.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT2.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT3.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT3.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT3.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT3.SEL == n/2.
- TRCSEQEVR<a>.B.TYPE == 0b0 and TRCSEQEVR<a>.B.SEL = n.
- TRCSEQEVR<a>.B.TYPE == 0b1 and TRCSEQEVR<a>.B.SEL = n/2.
- TRCSEQEVR<a>.F.TYPE == 0b0 and TRCSEQEVR<a>.F.SEL = n.
- TRCSEQEVR<a>.F.TYPE == 0b1 and TRCSEQEVR<a>.F.SEL = n/2.
- AArch64-TRCSEQRSTEV.RST.TYPE == 0b0 and AArch64-TRCSEQRSTEV.RST.SEL == n.
- AArch64-TRCSEQRSTEV.RST.TYPE == 0b1 and AArch64-TRCSEQRSTEV.RST.SEL == n/2.
- AArch64-TRCTSCTLR.EVENT.TYPE == 0b0 and AArch64-TRCTSCTLR.EVENT.SEL == n.
- AArch64-TRCTSCTLR.EVENT.TYPE == 0b1 and AArch64-TRCTSCTLR.EVENT.SEL == n/2.
- AArch64-TRCVICTLR.EVENT.TYPE == 0b0 and AArch64-TRCVICTLR.EVENT.SEL == n.
- AArch64-TRCVICTLR.EVENT.TYPE == 0b1 and AArch64-TRCVICTLR.EVENT.SEL == n/2.

MRS <Xt>, TRCRSCTLR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	m[3:0]	'00':m[4]

MSR TRCRSCTLR&lt;m&gt;, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b10	0b001	0b0001	m[3:0]	'00':m[4]

## Accessibility

Must be programmed if any of the following are true:

- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.RLDEVENT.SEL == n.
- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.RLDEVENT.SEL == n/2.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.CNTEVENT.SEL == n.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.CNTEVENT.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT0.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT0.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT0.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT0.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT1.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT1.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT1.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT1.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT2.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT2.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT2.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT2.SEL == n/2.
- AArch64-TRCEVENTCTLOR.EVENT3.TYPE == 0b0 and AArch64-TRCEVENTCTLOR.EVENT3.SEL == n.
- AArch64-TRCEVENTCTLOR.EVENT3.TYPE == 0b1 and AArch64-TRCEVENTCTLOR.EVENT3.SEL == n/2.
- TRCSEQEVR<a>.B.TYPE == 0b0 and TRCSEQEVR<a>.B.SEL = n.
- TRCSEQEVR<a>.B.TYPE == 0b1 and TRCSEQEVR<a>.B.SEL = n/2.
- TRCSEQEVR<a>.F.TYPE == 0b0 and TRCSEQEVR<a>.F.SEL = n.
- TRCSEQEVR<a>.F.TYPE == 0b1 and TRCSEQEVR<a>.F.SEL = n/2.
- AArch64-TRCSEQRSTEV.RST.TYPE == 0b0 and AArch64-TRCSEQRSTEV.RST.SEL == n.
- AArch64-TRCSEQRSTEV.RST.TYPE == 0b1 and AArch64-TRCSEQRSTEV.RST.SEL == n/2.
- AArch64-TRCTSCTLR.EVENT.TYPE == 0b0 and AArch64-TRCTSCTLR.EVENT.SEL == n.
- AArch64-TRCTSCTLR.EVENT.TYPE == 0b1 and AArch64-TRCTSCTLR.EVENT.SEL == n/2.
- AArch64-TRCVICTLR.EVENT.TYPE == 0b0 and AArch64-TRCVICTLR.EVENT.SEL == n.

- AArch64-TRCVICTLR.EVENT.TYPE == 0b1 and AArch64-TRCVICTLR.EVENT.SEL == n/2.  
MRS <Xt>, TRCRSCTLR<m>

```
integer m = UInt(op2<0>:CRm<3:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCRSCTLR[m];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCRSCTLR[m];
```

MSR TRCRSCTLR<m>, <Xt>

```
integer m = UInt(op2<0>:CRm<3:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCRSCTLR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCRSCTLR[m] = X[t, 64];
```

#### A.2.8.46 TRCDVCVR<n>, Data Value Comparator Value Register <n> , n = 0 - 1

Contains a data value.

##### Configurations

AArch64 register TRCDVCVR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.50 TRCDVCVR<n>, Data Value Comparator Value Register <n> , n = 0 - 1](#) on page 2175 bits [63:0].

##### Attributes

###### Width

64

###### Functional group

Trace unit registers

Access type  
See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-430: AARCH64\_TRCDVCVR<n> bit assignments

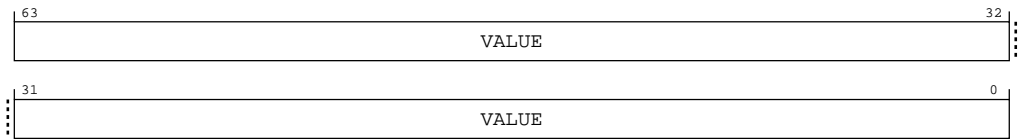


Table A-1100: TRCDVCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:0]	VALUE	Data Value.  The data value comparators can support implementations that use multiple data widths. When the trace unit compares the VALUE field with a data value that has a width less than this field, then software must also write the comparison data value to both the upper bits and the lower bits of the VALUE field. For example, in a system that supports both 32-bit and 64-bit data widths, then software must set VALUE[63:32]==VALUE[31:0] if the trace unit is to compare a 32-bit data value.	64 {x}

Access  
Might ignore writes when the trace unit is enabled or not idle.  
  
MRS <Xt>, TRCDVCVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[1:0] : '00'	'10' : m[2]

MSR TRCDVCVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[1:0] : '00'	'10' : m[2]

Accessibility  
Might ignore writes when the trace unit is enabled or not idle.

MRS &lt;Xt&gt;, TRCDVCVR&lt;m&gt;

```

integer m = UInt(op2<0>:CRm<3:2>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDVCVR[m];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDVCVR[m];

```

MSR TRCDVCVR&lt;m&gt;, &lt;Xt&gt;

```

integer m = UInt(op2<0>:CRm<3:2>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCDVCVR[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCDVCVR[m] = X[t, 64];

```

#### A.2.8.47 TRCDVCMR<n>, Data Value Comparator Mask Register <n> , n = 0 - 1

Contains a data mask value.

##### Configurations

AArch64 register TRCDVCMR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.51 TRCDVCMR<n>, Data Value Comparator Mask Register <n> , n = 0 - 1](#) on page 2177 bits [63:0].

##### Attributes

###### Width

64

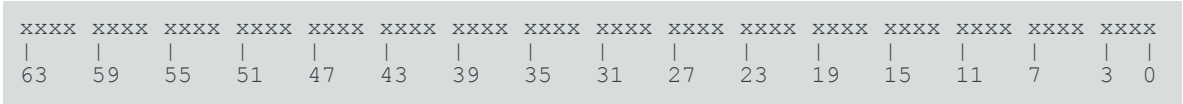
###### Functional group

Trace unit registers

###### Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-431: AArch64\_TRCDVCMR<n> bit assignments

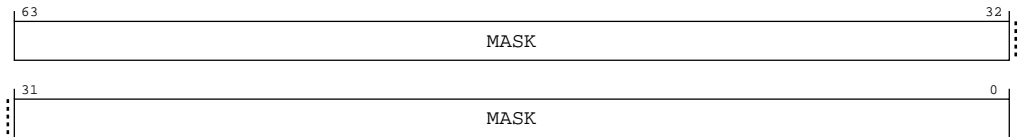


Table A-1103: TRCDVCMR<n> bit descriptions

Bits	Name	Description	Reset
[63:0]	MASK	<p>Data mask value.</p> <p>If a bit is set to 1 in the mask then the comparator ignores that bit number for a data value comparison. Software must ensure that the relevant bit in AArch64-TRCDVCVR&lt;n&gt; is programmed to 0, otherwise the comparator might fail to match.</p> <p>The data value comparators can support implementations that use multiple data widths. When the trace unit compares the AArch64-TRCDVCVR&lt;n&gt;.VALUE field with a data value that has a width less than this field, then software must also write the data mask value to both the upper bits and the lower bits of the MASK field. For example, in a system that supports both 32-bit and 64-bit data widths, then software must set MASK[63:32]=MASK[31:0] if the trace unit is to compare a 32-bit data value.</p>	64 {x}

Access

Might ignore writes when the trace unit is enabled or not idle.

MRS <Xt>, TRCDVCMR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[1:0]:'00'	'11':m[2]

MSR TRCDVCMR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[1:0]:'00'	'11':m[2]

## Accessibility

Might ignore writes when the trace unit is enabled or not idle.

MRS <Xt>, TRCDVCMR<m>

```

integer m = UInt(op2<0>:CRm<3:2>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDVCMR[m];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDVCMR[m];

```

MSR TRCDVCMR<m>, <Xt>

```

integer m = UInt(op2<0>:CRm<3:2>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCDVCMR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCDVCMR[m] = X[t, 64];

```

## A.2.8.48 TRCACVR<n>, Address Comparator Value Register <n> , n = 0 - 7

Contains the address value.

### Configurations

AArch64 register TRCACVR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.48 TRCACVR<n>, Address Comparator Value Register <n> , n = 0 - 7](#) on page 2168 bits [63:0].

### Attributes

#### Width

64

#### Functional group

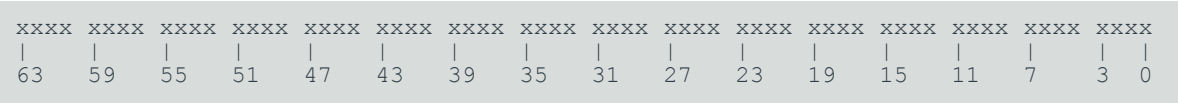
Trace unit registers



Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-432: AARCH64\_TRCACVR<n> bit assignments

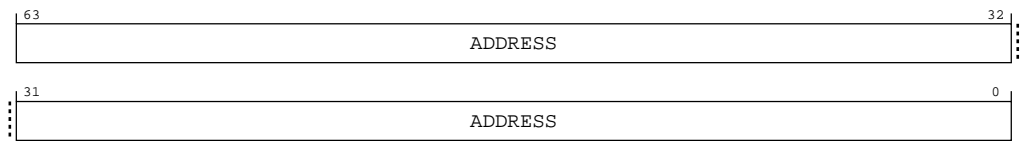


Table A-1106: TRCACVR<n> bit descriptions

Bits	Name	Description	Reset
[63:0]	ADDRESS	<p>Address Value.</p> <p>The address comparators can support implementations that use multiple address widths. When the trace unit compares the ADDRESS field with an address that has a width less than this field, then the address must be zero-extended to the ADDRESS field width. The trace unit then compares all implemented bits.</p> <p>The result of writing a value other than all zeros or all ones to ADDRESS at bits[63:P] is an <b>UNKNOWN</b> value, where P is defined as the virtual address size supported by the PE.</p> <p>The result of writing a value of all zeros or all ones to ADDRESS at bits[63:P] is the written value, and a read of the register returns the written value.</p>	64 {x}

Access

Must be programmed if any of the following are true:

- AArch64-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- AArch64-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- AArch64-TRCVIIECTLR.INCLUDE[n/2] == 0b1.

- AArch64-TRCVISSCTLR.START[n] == 0b1.
- AArch64-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- AArch64-TRCQCTLR.RANGE[n/2] == 0b1.

MRS <Xt>, TRCACVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[2:0]:'0'	'00':m[3]

MSR TRCACVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[2:0]:'0'	'00':m[3]

## Accessibility

Must be programmed if any of the following are true:

- AArch64-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- AArch64-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- AArch64-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- AArch64-TRCVISSCTLR.START[n] == 0b1.
- AArch64-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- AArch64-TRCQCTLR.RANGE[n/2] == 0b1.

MRS <Xt>, TRCACVR<m>

```
integer m = UInt(op2<0>:CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCACVR[m];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
```

```
else
    X[t, 64] = TRCACVR[m];
```

MSR TRCACVR<m>, <Xt>

```
integer m = UInt(op2<0>:CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCACVR[m] = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCACVR[m] = X[t, 64];
```

A.2.8.49 TRCACATR<n>, Address Comparator Access Type Register <n> , n = 0 - 7

Defines the type of access for the corresponding AArch64-TRCACVR<n> Register. This register configures the context type, Exception levels, alignment, masking that is applied by the address comparator, and how the address comparator behaves when it is one half of an Address Range Comparator.

Configurations

AArch64 register TRCACATR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.49 TRCACATR<n>, Address Comparator Access Type Register <n> , n = 0 - 7](#) on page 2171 bits [63:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

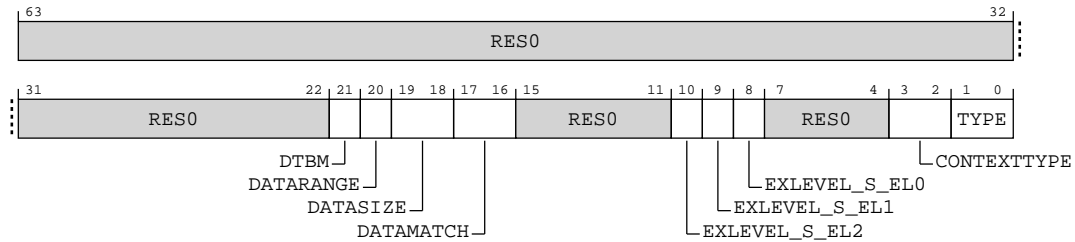
Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure A-433: AARCH64\_TRCACATR<n> bit assignments****Table A-1109: TRCACATR<n> bit descriptions**

Bits	Name	Description	Reset
[63:22]	RES0	Reserved	RES0
[21]	DTBM	Controls whether data address comparisons use the data address [63:56] bits.  <b>0b0</b> The trace unit ignores the data address [63:56] bits for data address comparisons.  <b>0b1</b> The trace unit uses the data address [63:56] bits for data address comparisons.	x
[20]	DATARANGE	Controls whether a data value comparison uses the single address comparator or the address range comparator.  <b>0b0</b> The trace unit uses the single address comparator for data value comparisons. The address range comparator may match at any time. The other single address comparator in the pair is not affected.  <b>0b1</b> The trace unit uses the address range comparator for data value comparisons. The single address comparators in this pair may match at any time.  The trace unit ignores this field when DATAMATCH==0b00.	x
[19:18]	DATASIZE	Controls the width of the data value comparison.  <b>0b00</b> Byte.  <b>0b01</b> Halfword.  <b>0b10</b> Word.  <b>0b11</b> Doubleword.	xx

Bits	Name	Description	Reset
[17:16]	DATAMATCH	Controls how the trace unit performs a data value comparison.  <b>0b00</b> The trace unit does not perform a data value comparison.  <b>0b01</b> The trace unit performs a data value comparison. If the data value comparator matches and the address comparator matches, the trace unit signals a match.  <b>0b10</b> Reserved.  <b>0b11</b> The trace unit performs a data value comparison. If the data value comparator does not match and the address comparator matches, the trace unit signals a match.	xx
[15:11]	RES0	Reserved	RES0
[10]	EXLEVEL_S_EL2	Secure EL2 address comparison control. Controls whether a comparison can occur at EL2 in Secure state.  <b>0b0</b> The address comparator performs comparisons in Secure EL2.  <b>0b1</b> The address comparator does not perform comparisons in Secure EL2.	x
[9]	EXLEVEL_S_EL1	Secure EL1 address comparison control. Controls whether a comparison can occur at EL1 in Secure state.  <b>0b0</b> The address comparator performs comparisons in Secure EL1.  <b>0b1</b> The address comparator does not perform comparisons in Secure EL1.	x
[8]	EXLEVEL_S_ELO	Secure ELO address comparison control. Controls whether a comparison can occur at ELO in Secure state.  <b>0b0</b> The address comparator performs comparisons in Secure ELO.  <b>0b1</b> The address comparator does not perform comparisons in Secure ELO.	x
[7:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3:2]	CONTEXTTYPE	<p>Controls whether the address comparator is dependent on a Context Identifier Comparator, a Virtual Context Identifier Comparator, or both comparisons.</p> <p><b>0b00</b></p> <p>The address comparator is not dependent on the Context Identifier Comparator or Virtual Context Identifier Comparator.</p> <p><b>0b01</b></p> <p>The address comparator is dependent on the Context Identifier Comparator. If both the Context Identifier Comparator and the address comparison match, the address comparator signals a match.</p> <p><b>0b10</b></p> <p>The address comparator is dependent on the Virtual Context Identifier Comparator. If both the Virtual Context Identifier Comparator and the address comparison match, the address comparator signals a match.</p> <p><b>0b11</b></p> <p>The address comparator is dependent on the Context Identifier Comparator and Virtual Context Identifier Comparator. If the Context Identifier Comparator, the Virtual Context Identifier Comparator and address comparison all match, the address comparator signals a match.</p>	xx
[1:0]	TYPE	<p>Controls what type of comparison the trace unit performs.</p> <p><b>0b00</b></p> <p>Instruction address.</p> <p><b>0b01</b></p> <p>Data load address.</p> <p><b>0b10</b></p> <p>Data store address.</p> <p><b>0b11</b></p> <p>Data load address or data store address.</p>	xx

## Access

Must be programmed if any of the following are true:

- AArch64-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- AArch64-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- AArch64-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- AArch64-TRCVISSCTLR.START[n] == 0b1.
- AArch64-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.

- AArch64-TRCQCTLR.RANGE[n/2] == 0b1.

MRS <Xt>, TRCACATR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[2:0]:'0'	'01':m[3]

MSR TRCACATR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0010	m[2:0]:'0'	'01':m[3]

### Accessibility

Must be programmed if any of the following are true:

- AArch64-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- AArch64-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- AArch64-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- AArch64-TRCVISSCTLR.START[n] == 0b1.
- AArch64-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- AArch64-TRCQCTLR.RANGE[n/2] == 0b1.

MRS <Xt>, TRCACATR<m>

```
integer m = UInt(op2<0>:CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCACATR[m];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCACATR[m];
```

MSR TRCACATR<m>, <Xt>

```
integer m = UInt(op2<0>:CRm<3:1>);

if PSTATE.EL == EL0 then
```

```
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCACATR[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCACATR[m] = X[t, 64];
```

A.2.8.50 TRCCIDCCTLRO, Context Identifier Comparator Control Register 0

Contains Context identifier mask values for the AArch64-TRCCIDCVR<n> registers, for n = 0 to 3.

Configurations

AArch64 register TRCCIDCCTLRO bits [31:0] are architecturally mapped to External register [B.2.2.7.54 TRCCIDCCTLRO, Context Identifier Comparator Control Register 0](#) on page 2181 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-434: AARCH64\_TRCCIDCCTLR0 bit assignments

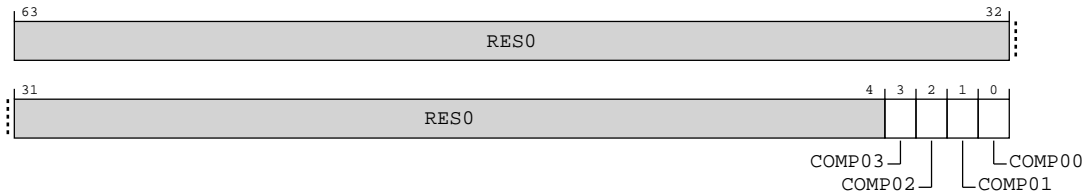


Table A-1112: TRCCIDCCTLR0 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	COMP0<m>, bit[m], where m = 3 to 0	TRCCIDCVR0 mask control. Specifies the mask value that the trace unit applies to TRCCIDCVR0. Each bit in this field corresponds to a byte in TRCCIDCVR0.  <b>0b0</b> The trace unit includes TRCCIDCVR0[(m×8+7):(m×8)] when it performs the Context identifier comparison.  <b>0b1</b> The trace unit ignores TRCCIDCVR0[(m×8+7):(m×8)] when it performs the Context identifier comparison.	xxxx

Access

If software uses the AArch64-TRCCIDCVR<n> registers, for n = 0 to 3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in AArch64-TRCCIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in AArch64-TRCCIDCVR<n> is not 0x00, the Context Identifier Comparator will not match.

MRS <Xt>, TRCCIDCCTLR0

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	0b0000	0b010

MSR TRCCIDCCTLR0, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	0b0000	0b010

Accessibility

If software uses the AArch64-TRCCIDCVR<n> registers, for n = 0 to 3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in AArch64-TRCCIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in AArch64-TRCCIDCVR<n> is not 0x00, the Context Identifier Comparator will not match.

MRS <Xt>, TRCCIDCCTLRO

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCIDCCTLRO;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCIDCCTLRO;
```

MSR TRCCIDCCTLRO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCIDCCTLRO = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCIDCCTLRO = X[t, 64];
```

### A.2.8.51 TRCVMIDCCTLRO, Virtual Context Identifier Comparator Control Register 0

Virtual Context Identifier Comparator mask values for the AArch64-TRCVMIDCVR<n> registers, where n=0-3.

#### Configurations

AArch64 register TRCVMIDCCTLRO bits [31:0] are architecturally mapped to External register [B.2.2.7.55 TRCVMIDCCTLRO, Virtual Context Identifier Comparator Control Register 0](#) on page 2183 bits [31:0].

#### Attributes

##### Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-435: AARCH64\_TRCVMIDCCTLR0 bit assignments

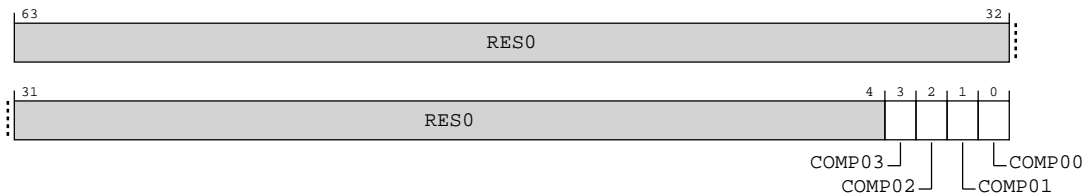


Table A-1115: TRCVMIDCCTLR0 bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	COMP0<m>, bit[m], where m = 3 to 0	<p>TRCVMIDCVR0 mask control. Specifies the mask value that the trace unit applies to TRCVMIDCVR0. Each bit in this field corresponds to a byte in TRCVMIDCVR0.</p> <p><b>0b0</b></p> <p>The trace unit includes TRCVMIDCVR0[(m×8+7):(m×8)] when it performs the Virtual context identifier comparison.</p> <p><b>0b1</b></p> <p>The trace unit ignores TRCVMIDCVR0[(m×8+7):(m×8)] when it performs the Virtual context identifier comparison.</p>	xxxx

Access

If software uses the AArch64-TRCVMIDCVR<n> registers, where n=0-3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in AArch64-TRCVMIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in AArch64-TRCVMIDCVR<n> is not 0x00, the Virtual Context Identifier Comparator will not match.

MRS <Xt>, TRCVMIDCCTLRO

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	0b0010	0b010

MSR TRCVMIDCCTLRO, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	0b0010	0b010

Accessibility

If software uses the AArch64-TRCVMIDCVR<n> registers, where n=0-3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in AArch64-TRCVMIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in AArch64-TRCVMIDCVR<n> is not 0x00, the Virtual Context Identifier Comparator will not match.

MRS <Xt>, TRCVMIDCCTLRO

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVMIDCCTLRO;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVMIDCCTLRO;
```

MSR TRCVMIDCCTLRO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVMIDCCTLRO = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVMIDCCTLRO = X[t, 64];
```

A.2.8.52 TRCCIDCVR<n>, Context Identifier Comparator Value Registers <n> , n = 0

Contains a Context identifier value.

Configurations

AArch64 register TRCCIDCVR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.52 TRCCIDCVR<n>, Context Identifier Comparator Value Registers <n> , n = 0](#) on page 2178 bits [63:0].

Attributes

Width

64

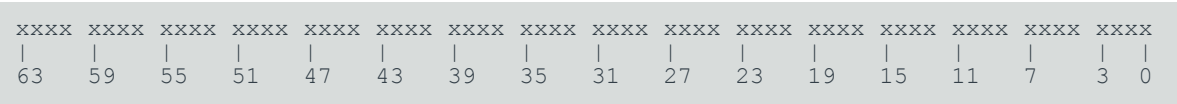
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-436: AARCH64\_TRCCIDCVR<n> bit assignments

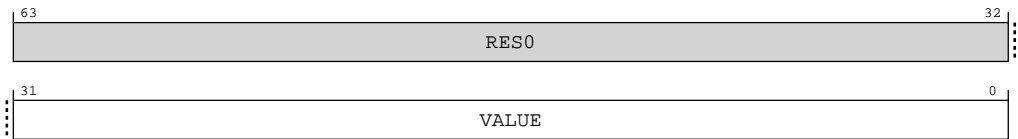


Table A-1118: TRCCIDCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	VALUE	Context identifier value. After a PE Reset, the trace unit assumes that the Context identifier is zero until the PE updates the Context identifier.	32 {x}

## Access

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0110 and TRCRSCTLR<a>.CID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b01 or 0b11 and TRCACATR<a>.CONTEXT == n.

MRS <Xt>, TRCCIDCVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	m[2:0]:'0'	0b000

MSR TRCCIDCVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	m[2:0]:'0'	0b000

## Accessibility

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0110 and TRCRSCTLR<a>.CID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b01 or 0b11 and TRCACATR<a>.CONTEXT == n.

MRS <Xt>, TRCCIDCVR<m>

```

integer m = UInt(CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCIDCVR[m];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCCIDCVR[m];

```

MSR TRCCIDCVR<m>, <Xt>

```

integer m = UInt(CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCIDCVR[m] = X[t, 64];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then

```

```
AArch64.SystemAccessTrap(EL2, 0x18);
else
    TRCCIDCVR[m] = X[t, 64];
```

A.2.8.53 TRCVMIDCVR<n>, Virtual Context Identifier Comparator Value Register <n> , n = 0

Contains the Virtual Context Identifier Comparator value.

Configurations

AArch64 register TRCVMIDCVR<n> bits [63:0] are architecturally mapped to External register [B.2.2.7.53 TRCVMIDCVR<n>, Virtual Context Identifier Comparator Value Register <n> , n = 0](#) on page 2180 bits [63:0].

Attributes

Width

64

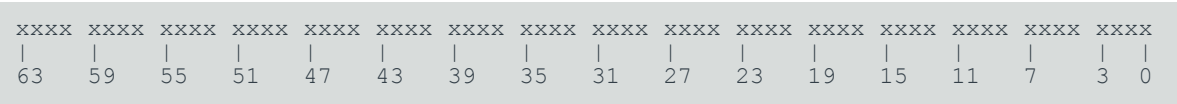
Functional group

Trace unit registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-437: AARCH64\_TRCVMIDCVR<n> bit assignments

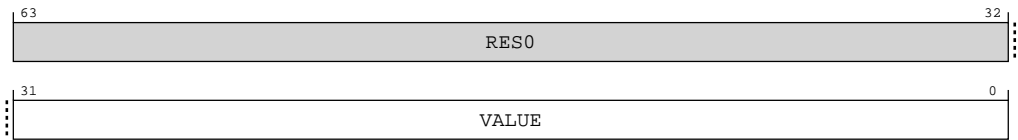


Table A-1121: TRCVMIDCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[31:0]	VALUE	Virtual context identifier value. After a PE Reset, the trace unit assumes that the Virtual context identifier is zero until the PE updates the Virtual context identifier.	32 {x}

### Access

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0111 and TRCRSCTLR<a>.VMID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b10 or 0b11 and TRCACATR<a>.CONTEXT == n.

MRS <Xt>, TRCVMIDCVR<m>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	m[2:0]:'0'	0b001

MSR TRCVMIDCVR<m>, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0011	m[2:0]:'0'	0b001

### Accessibility

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0111 and TRCRSCTLR<a>.VMID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b10 or 0b11 and TRCACATR<a>.CONTEXT == n.

MRS <Xt>, TRCVMIDCVR<m>

```
integer m = UInt(CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCVMIDCVR[m];
    elsif PSTATE.EL == EL2 then
        if CPTR_EL2.TTA == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = TRCVMIDCVR[m];
```

MSR TRCVMIDCVR<m>, <Xt>

```
integer m = UInt(CRm<3:1>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
```



```
elseif CPTR_EL2.TTA == '1' then
    AArch64.SystemAccessTrap(EL2, 0x18);
else
    TRCVMIDCVR[m] = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCVMIDCVR[m] = X[t, 64];
```

A.2.8.54 TRCDEVID, Device Configuration Register

Provides discovery information for the component.

Configurations

AArch64 register TRCDEVID bits [31:0] are architecturally mapped to External register [B.2.2.7.64 TRCDEVID, Device Configuration Register](#) on page 2195 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-438: AARCH64\_TRCDEVID bit assignments

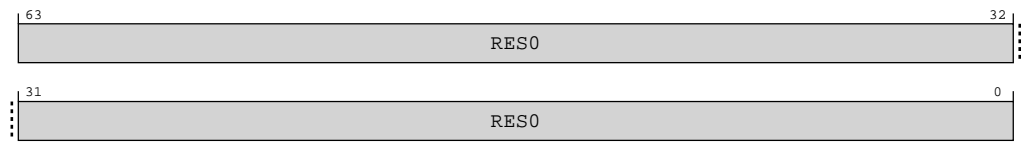


Table A-1124: TRCDEVID bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

**Access**  
MRS <Xt>, TRCDEVID

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b0010	0b111

**Accessibility**  
MRS <Xt>, TRCDEVID

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDEVID;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDEVID;
```

A.2.8.55 TRCCLAIMSET, Claim Tag Set Register

In conjunction with AArch64-TRCCLAIMCLR, provides Claim Tag bits that can be separately set and cleared to indicate whether functionality is in use by a debug agent.

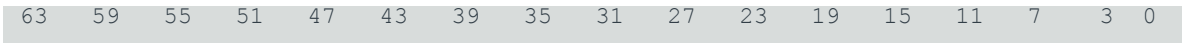
Configurations

AArch64 register TRCCLAIMSET bits [31:0] are architecturally mapped to External register [B.2.2.7.57 TRCCLAIMSET, Claim Tag Set Register](#) on page 2186 bits [31:0].

Attributes

- Width**  
64
- Functional group**  
Trace unit registers
- Access type**  
RAOW1S
- Reset value**





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-439: AARCH64\_TRCCLAIMSET bit assignments

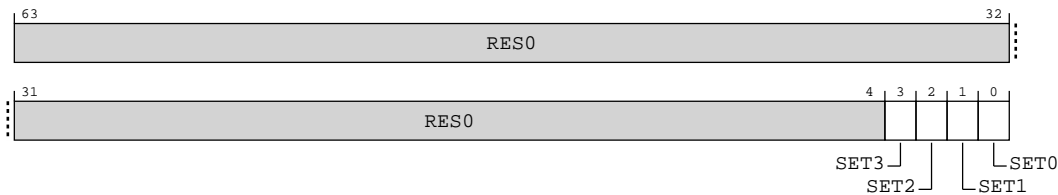


Table A-1126: TRCCLAIMSET bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	SET<m>, bit[m], where m = 3 to 0	<div>Claim Tag Set. Indicates whether Claim Tag bit m is implemented, and is used to set Claim Tag bit m to 0b1.</div> <div><b>0b0</b> On a read: Claim Tag bit m is not implemented. On a write: Ignored.</div> <div><b>0b1</b> On a read: Claim Tag bit m is implemented. On a write: Set Claim Tag bit m to 0b1.</div>	0b1111

Access

MRS <Xt>, TRCCLAIMSET

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1000	0b110

MSR TRCCLAIMSET, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1000	0b110

## Accessibility

MRS <Xt>, TRCCLAIMSET

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCLAIMSET;
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCLAIMSET;

```

MSR TRCCLAIMSET, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elsif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCLAIMSET = X[t, 64];
elsif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCLAIMSET = X[t, 64];

```

### A.2.8.56 TRCCLAIMCLR, Claim Tag Clear Register

In conjunction with AArch64-TRCCLAIMSET, provides Claim Tag bits that can be separately set and cleared to indicate whether functionality is in use by a debug agent.

#### Configurations

AArch64 register TRCCLAIMCLR bits [31:0] are architecturally mapped to External register [B.2.2.7.58 TRCCLAIMCLR, Claim Tag Clear Register](#) on page 2187 bits [31:0].

#### Attributes

##### Width

64

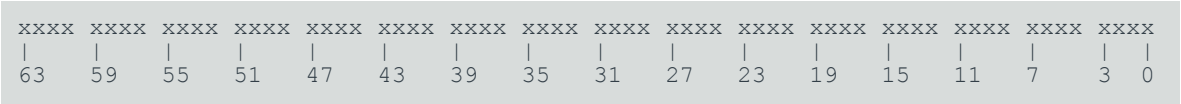
##### Functional group

Trace unit registers

##### Access type

RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-440: AARCH64\_TRCCLAIMCLR bit assignments

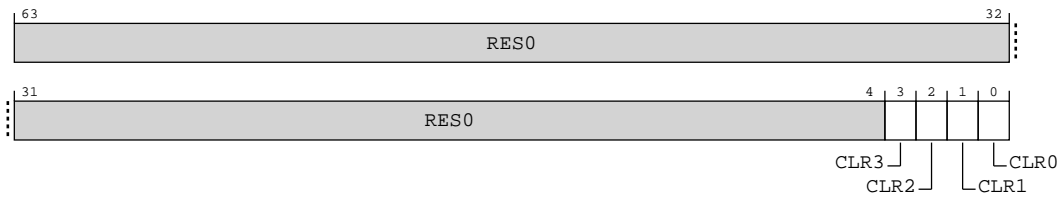


Table A-1129: TRCCLAIMCLR bit descriptions

Bits	Name	Description	Reset
[63:4]	RES0	Reserved	RES0
[3:0]	CLR<m>, bit[m], where m = 3 to 0	<p>Claim Tag Clear. Indicates the current status of the Claim Tag bit m, and is used to clear Claim Tag bit m to 0b0.</p> <p><b>0b0</b></p> <p>On a read: Claim Tag bit m is not set.</p> <p>On a write: Ignored.</p> <p><b>0b1</b></p> <p>On a read: Claim Tag bit m is set.</p> <p>On a write: Clear Claim tag bit m to 0b0.</p> <p>The number of Claim Tag bits implemented is indicated in AArch64-TRCCLAIMSET.</p>	xxxx

Access

MRS <Xt>, TRCCLAIMCLR

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1001	0b110

MSR TRCCLAIMCLR, <Xt>

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1001	0b110

## Accessibility

MRS <Xt>, TRCCLAIMCLR

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCLAIMCLR;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCCLAIMCLR;

```

MSR TRCCLAIMCLR, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCLAIMCLR = X[t, 64];
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        TRCCLAIMCLR = X[t, 64];

```

### A.2.8.57 TRCAUTHSTATUS, Authentication Status Register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for debug.

## Configurations

AArch64 register TRCAUTHSTATUS bits [31:0] are architecturally mapped to External register [B.2.2.7.62 TRCAUTHSTATUS, Authentication Status Register](#) on page 2192 bits [31:0].

## Attributes

### Width

64

### Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00	0000
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-441: AARCH64\_TRCAUTHSTATUS bit assignments

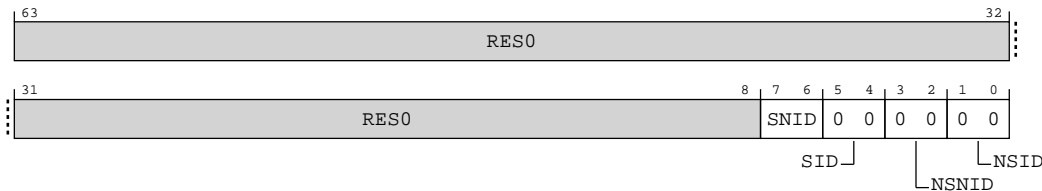


Table A-1132: TRCAUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure Non-invasive Debug. Indicates whether Secure non-invasive debug features are implemented and enabled.  <b>0b10</b> Secure Non-invasive Debug implemented and disabled.  <b>0b11</b> Secure Non-invasive Debug implemented and enabled.	xx
[5:4]	SID	Secure Invasive Debug. Indicates whether Secure invasive debug features are implemented and enabled.  <b>0b00</b> Secure invasive debug features not implemented.	0b00
[3:2]	NSNID	Non-secure Non-invasive Debug. Indicates whether Non-secure non-invasive debug features are implemented and enabled.  <b>0b00</b> Non-secure non-invasive debug features not implemented.	0b00
[1:0]	NSID	Non-secure Invasive Debug. Indicates whether Non-secure invasive debug features are implemented and enabled.  <b>0b00</b> Non-secure invasive debug features not implemented.	0b00

Access

MRS <Xt>, TRCAUTHSTATUS

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1110	0b110

Accessibility

MRS <Xt>, TRCAUTHSTATUS

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCAUTHSTATUS;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCAUTHSTATUS;
```

A.2.8.58 TRCDEVARCH, Device Architecture Register

Provides discovery information for the component.

Configurations

AArch64 register TRCDEVARCH bits [31:0] are architecturally mapped to External register [B.2.2.7.63 TRCDEVARCH, Device Architecture Register](#) on page 2194 bits [31:0].

Attributes

Width

64

Functional group

Trace unit registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0100	0111	0111	0101	0100	1010	0001	0011
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-442: AARCH64\_TRCDEVARCH bit assignments

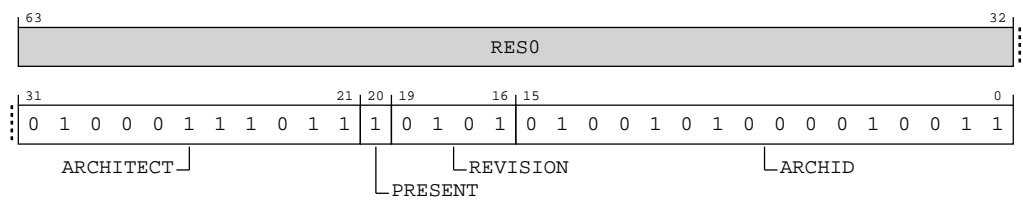


Table A-1134: TRCDEVARCH bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:21]	ARCHITECT	Architect. Defines the architect of the component. <b>0b01000111011</b> JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	DEVARCH Present. Defines that the DEVARCH register is present. <b>0b1</b> Device Architecture information present.	0b1
[19:16]	REVISION	Revision. Defines the architecture revision of the component. <b>0b0101</b> ETMv4.5.	0b0101
[15:0]	ARCHID	Architecture ID. <b>0b0100101000010011</b> Arm PE Trace architecture ETMv4.	0x4A13

Access  
MRS <Xt>, TRCDEVARCH

op0	op1	CRn	CRm	op2
0b10	0b001	0b0111	0b1111	0b110

Accessibility  
MRS <Xt>, TRCDEVARCH

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if CPACR_EL1.TTA == '1' then
        AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = TRCDEVARCH;
elseif PSTATE.EL == EL2 then
    if CPTR_EL2.TTA == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

X[t, 64] = TRCDEVARCH;

### A.2.9 AArch64 Special purpose register description

This section includes the register descriptions for all Special purpose registers in the Cortex®-R82AE processor.

#### A.2.9.1 SPSR\_EL1, Saved Program Status Register (EL1)

Holds the saved process state when an exception is taken to EL1.

##### Configurations

This register is available in all configurations.

##### Attributes

###### Width

64

###### Functional group

Special-purpose registers

###### Access type

See bit descriptions

###### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

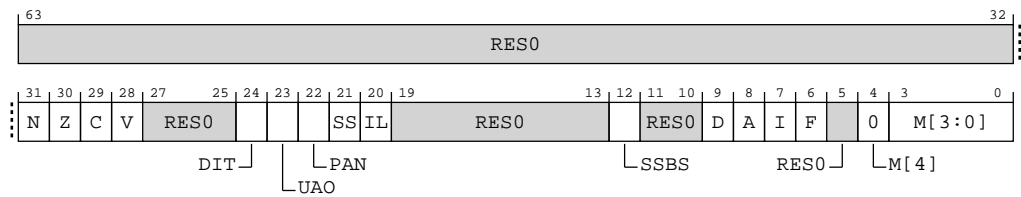


Where the reset reads xxxx, see individual bits.

##### Bit descriptions

An exception return from EL1 using AArch64 makes SPSR\_EL1 become **UNKNOWN**.

Figure A-443: AARCH64\_SPSR\_EL1 bit assignments



**Table A-1136: SPSR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31]	N	Negative Condition flag. Set to the value of PSTATE.N on taking an exception to EL1, and copied to PSTATE.N on executing an exception return operation in EL1.	x
[30]	Z	Zero Condition flag. Set to the value of PSTATE.Z on taking an exception to EL1, and copied to PSTATE.Z on executing an exception return operation in EL1.	x
[29]	C	Carry Condition flag. Set to the value of PSTATE.C on taking an exception to EL1, and copied to PSTATE.C on executing an exception return operation in EL1.	x
[28]	V	Overflow Condition flag. Set to the value of PSTATE.V on taking an exception to EL1, and copied to PSTATE.V on executing an exception return operation in EL1.	x
[27:25]	<b>RES0</b>	Reserved	<b>RES0</b>
[24]	DIT	Data Independent Timing. Set to the value of PSTATE.DIT on taking an exception to EL1, and copied to PSTATE.DIT on executing an exception return operation in EL1.	x
[23]	UAO	User Access Override. Set to the value of PSTATE.UAO on taking an exception to EL1, and copied to PSTATE.UAO on executing an exception return operation in EL1.	x
[22]	PAN	Privileged Access Never. Set to the value of PSTATE.PAN on taking an exception to EL1, and copied to PSTATE.PAN on executing an exception return operation in EL1.	x
[21]	SS	Software Step. Set to the value of PSTATE.SS on taking an exception to EL1, and conditionally copied to PSTATE.SS on executing an exception return operation in EL1.	x
[20]	IL	Illegal Execution state. Set to the value of PSTATE.IL on taking an exception to EL1, and copied to PSTATE.IL on executing an exception return operation in EL1.	x
[19:13]	<b>RES0</b>	Reserved	<b>RES0</b>
[12]	SSBS	Speculative Store Bypass. Set to the value of PSTATE.SSBS on taking an exception to EL1, and copied to PSTATE.SSBS on executing an exception return operation in EL1.	x
[11:10]	<b>RES0</b>	Reserved	<b>RES0</b>
[9]	D	Debug exception mask. Set to the value of PSTATE.D on taking an exception to EL1, and copied to PSTATE.D on executing an exception return operation in EL1.	x
[8]	A	SError interrupt mask. Set to the value of PSTATE.A on taking an exception to EL1, and copied to PSTATE.A on executing an exception return operation in EL1.	x
[7]	I	IRQ interrupt mask. Set to the value of PSTATE.I on taking an exception to EL1, and copied to PSTATE.I on executing an exception return operation in EL1.	x
[6]	F	FIQ interrupt mask. Set to the value of PSTATE.F on taking an exception to EL1, and copied to PSTATE.F on executing an exception return operation in EL1.	x
[5]	<b>RES0</b>	Reserved	<b>RES0</b>
[4]	M[4]	Execution state. Set to 0b0, the value of PSTATE.nRW, on taking an exception to EL1 from AArch64 state, and copied to PSTATE.nRW on executing an exception return operation in EL1.  <b>0b0</b> AArch64 execution state.	0b0

Bits	Name	Description	Reset
[3:0]	M[3:0]	<p>AArch64 Exception level and selected Stack Pointer.</p> <p><b>0b0000</b> EL0t.</p> <p><b>0b0100</b> EL1t.</p> <p><b>0b0101</b> EL1h.</p> <p>Other values are reserved. If SPSR_EL1.M[3:0] has a Reserved value, or a value for an unimplemented Exception level, executing an exception return operation in EL1 is an illegal return event, as described in <i>Illegal return events from AArch64 state</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>The bits in this field are interpreted as follows:</p> <ul style="list-style-type: none"> <li>M[3:2]: On an exception to EL1: <ul style="list-style-type: none"> <li>If the Effective value of AArch64-HCR_EL2.{NV, NV1} != {1,0} or the exception is not taken from EL1, then M[3:2] is set to the value of PSTATE.EL on taking an exception to EL1.</li> <li>If the Effective value of AArch64-HCR_EL2.{NV, NV1} == {1,0} and the exception is not taken from EL1, then M[3:2] is set to 0b10.</li> <li>M[3:2] is copied to PSTATE.EL on executing a legal exception return operation in EL1.</li> </ul> </li> <li>M[1] is unused and is 0 for all non-reserved values.</li> <li>M[0] is set to the value of PSTATE.SP on taking an exception to EL1 and copied to PSTATE.SP on executing an exception return operation in EL1.</li> </ul>	xxxx

## Access

MRS <Xt>, SPSR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0000	0b000

MSR SPSR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0000	0b000

## Accessibility

MRS <Xt>, SPSR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = SPSR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_EL1;

```

MSR SPSR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then

```

```
    UNDEFINED;
    elsif PSTATE.EL == EL1 then
        SPSR_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        SPSR_EL1 = X[t, 64];
```

A.2.9.2 ELR\_EL1, Exception Link Register (EL1)

When taking an exception to EL1, holds the address to return to.

Configurations

This register is available in all configurations.

Attributes

Width

64

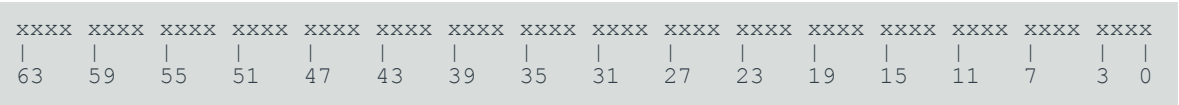
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-444: AARCH64\_EL1 bit assignments

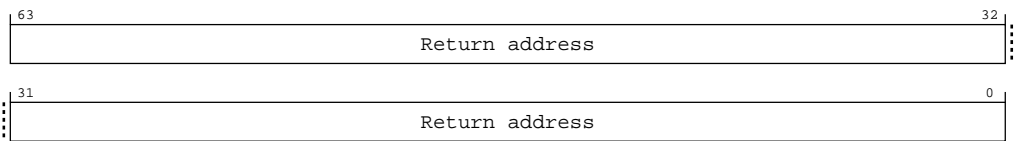


Table A-1139: ELR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Return address.  An exception return from EL1 using AArch64 makes ELR_EL1 become <b>UNKNOWN</b> .	64 { x }

Access

MRS <Xt>, ELR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0000	0b001

MSR ELR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0000	0b001

Accessibility

MRS <Xt>, ELR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    X[t, 64] = ELR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ELR_EL1;
```

MSR ELR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    ELR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    ELR_EL1 = X[t, 64];
```

A.2.9.3 SP\_ELO, Stack Pointer (ELO)

Holds the stack pointer associated with EL0. At higher Exception levels, this is used as the current stack pointer when the value of AArch64-SPSel.SP is 0.

Configurations

This register is available in all configurations.

Attributes

Width

64

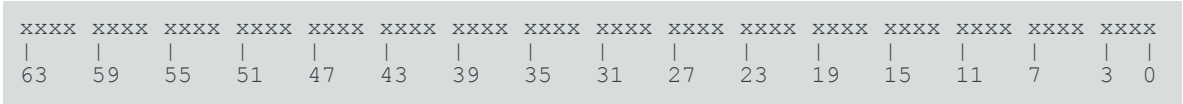
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-445: AARCH64\_SP\_ELO bit assignments

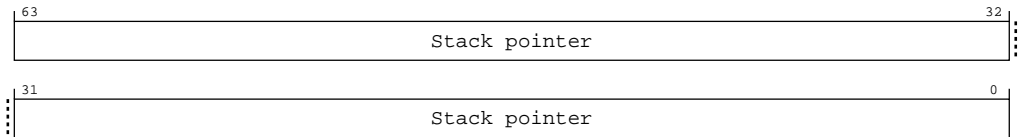


Table A-1142: SP\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Stack pointer.	64 {x}

Access

When the value of PSTATE.SP is 0, this register is accessible at all Exception levels as the current stack pointer.

MRS <Xt>, SP\_ELO

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0001	0b000

MSR SP\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0100	0b0001	0b000

Accessibility

When the value of PSTATE.SP is 0, this register is accessible at all Exception levels as the current stack pointer.

MRS <Xt>, SP\_ELO

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if PSTATE.SP == '0' then
```

```
        UNDEFINED;
    else
        X[t, 64] = SP_ELO;
    elsif PSTATE.EL == EL2 then
        if PSTATE.SP == '0' then
            UNDEFINED;
        else
            X[t, 64] = SP_ELO;
```

MSR SP\_ELO, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if PSTATE.SP == '0' then
        UNDEFINED;
    else
        SP_ELO = X[t, 64];
elsif PSTATE.EL == EL2 then
    if PSTATE.SP == '0' then
        UNDEFINED;
    else
        SP_ELO = X[t, 64];
```

A.2.9.4 DSPSR\_ELO, Debug Saved Program Status Register

Holds the saved process state for Debug state. On entering Debug state, PSTATE information is written to this register. On exiting Debug state, values are copied from this register to PSTATE.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

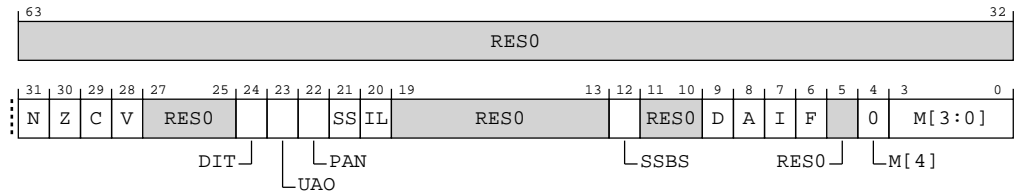


Where the reset reads xxxx, see individual bits.



## Bit descriptions

**Figure A-446: AARCH64\_DSPSR\_ELO bit assignments**



**Table A-1145: DSPSR\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31]	N	Negative Condition flag. Set to the value of PSTATE.N on entering Debug state, and copied to PSTATE.N on exiting Debug state.	x
[30]	Z	Zero Condition flag. Set to the value of PSTATE.Z on entering Debug state, and copied to PSTATE.Z on exiting Debug state.	x
[29]	C	Carry Condition flag. Set to the value of PSTATE.C on entering Debug state, and copied to PSTATE.C on exiting Debug state.	x
[28]	V	Overflow Condition flag. Set to the value of PSTATE.V on entering Debug state, and copied to PSTATE.V on exiting Debug state.	x
[27:25]	<b>RES0</b>	Reserved	<b>RES0</b>
[24]	DIT	Data Independent Timing. Set to the value of PSTATE.DIT on entering Debug state, and copied to PSTATE.DIT on exiting Debug state.	x
[23]	UAO	User Access Override. Set to the value of PSTATE.UAO on entering Debug state, and copied to PSTATE.UAO on exiting Debug state.	x
[22]	PAN	Privileged Access Never. Set to the value of PSTATE.PAN on entering Debug state, and copied to PSTATE.PAN on exiting Debug state.	x
[21]	SS	Software Step. Set to the value of PSTATE.SS on entering Debug state, and conditionally copied to PSTATE.SS on exiting Debug state.	x
[20]	IL	Illegal Execution state. Set to the value of PSTATE.IL on entering Debug state, and copied to PSTATE.IL on exiting Debug state.	x
[19:13]	<b>RES0</b>	Reserved	<b>RES0</b>
[12]	SSBS	Speculative Store Bypass. Set to the value of PSTATE.SSBS on entering Debug state, and copied to PSTATE.SSBS on exiting Debug state.	x
[11:10]	<b>RES0</b>	Reserved	<b>RES0</b>
[9]	D	Debug exception mask. Set to the value of PSTATE.D on entering Debug state, and copied to PSTATE.D on exiting Debug state.	x
[8]	A	SError interrupt mask. Set to the value of PSTATE.A on entering Debug state, and copied to PSTATE.A on exiting Debug state.	x
[7]	I	IRQ interrupt mask. Set to the value of PSTATE.I on entering Debug state, and copied to PSTATE.I on exiting Debug state.	x
[6]	F	FIQ interrupt mask. Set to the value of PSTATE.F on entering Debug state, and copied to PSTATE.F on exiting Debug state.	x
[5]	<b>RES0</b>	Reserved	<b>RES0</b>

Bits	Name	Description	Reset
[4]	M[4]	Execution state. Set to 0b0, the value of PSTATE.nRW, on entering Debug state from AArch64 state, and copied to PSTATE.nRW on exiting Debug state.  0b0 AArch64 execution state.	0b0
[3:0]	M[3:0]	AArch64 Exception level and selected Stack Pointer.  0b0000 EL0t.  0b0100 EL1t.  0b0101 EL1h.  0b1000 EL2t.  0b1001 EL2h.  Other values are reserved. If DSPSR_ELO.M[3:0] has a Reserved value, or a value for an unimplemented Exception level, exiting Debug state is an illegal return event, as described in <i>Illegal return events from AArch64 state</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .  The bits in this field are interpreted as follows: <ul style="list-style-type: none"> <li>M[3:2] is set to the value of PSTATE.EL on entering Debug state and copied to PSTATE.EL on exiting Debug state.</li> <li>M[1] is unused and is 0 for all non-reserved values.</li> <li>M[0] is set to the value of PSTATE.SP on entering Debug state and copied to PSTATE.SP on exiting Debug state.</li> </ul>	xxxx

## Access

MRS <Xt>, DSPSR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0101	0b000

MSR DSPSR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0101	0b000

## Accessibility

MRS <Xt>, DSPSR\_ELO

```

if !Halted() then
    UNDEFINED;
else
    X[t, 64] = DSPSR_ELO;

```

MSR DSPSR\_ELO, <Xt>

```
if !Halted() then
    UNDEFINED;
else
    DSPSR_ELO = X[t, 64];
```

A.2.9.5 DLR\_ELO, Debug Link Register

In Debug state, holds the address to restart from.

Configurations

This register is available in all configurations.

Attributes

Width

64

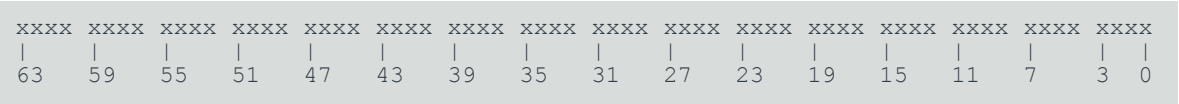
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-447: AARCH64\_DLR\_ELO bit assignments

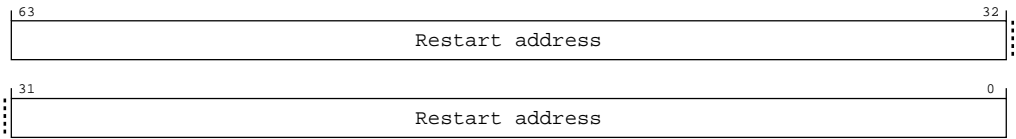


Table A-1148: DLR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Restart address.	64 {x}

Access

MRS <Xt>, DLR\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0101	0b001

MSR DLR\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b0100	0b0101	0b001

Accessibility

MRS <Xt>, DLR\_ELO

```
if !Halted() then
    UNDEFINED;
else
    X[t, 64] = DLR_ELO;
```

MSR DLR\_ELO, <Xt>

```
if !Halted() then
    UNDEFINED;
else
    DLR_ELO = X[t, 64];
```

A.2.9.6 SPSR\_EL2, Saved Program Status Register (EL2)

Holds the saved process state when an exception is taken to EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

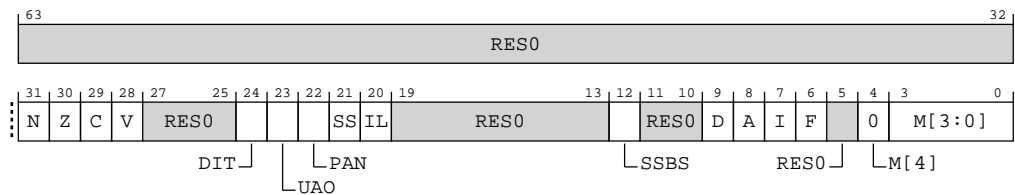


Where the reset reads xxxx, see individual bits.

## Bit descriptions

An exception return from EL2 using AArch64 makes SPSR\_EL2 become **UNKNOWN**.

**Figure A-448: AARCH64\_SPSR\_EL2 bit assignments**



**Table A-1151: SPSR\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31]	N	Negative Condition flag. Set to the value of PSTATE.N on taking an exception to EL2, and copied to PSTATE.N on executing an exception return operation in EL2.	x
[30]	Z	Zero Condition flag. Set to the value of PSTATE.Z on taking an exception to EL2, and copied to PSTATE.Z on executing an exception return operation in EL2.	x
[29]	C	Carry Condition flag. Set to the value of PSTATE.C on taking an exception to EL2, and copied to PSTATE.C on executing an exception return operation in EL2.	x
[28]	V	Overflow Condition flag. Set to the value of PSTATE.V on taking an exception to EL2, and copied to PSTATE.V on executing an exception return operation in EL2.	x
[27:25]	<b>RES0</b>	Reserved	<b>RES0</b>
[24]	DIT	Data Independent Timing. Set to the value of PSTATE.DIT on taking an exception to EL2, and copied to PSTATE.DIT on executing an exception return operation in EL2.	x
[23]	UAO	User Access Override. Set to the value of PSTATE.UAO on taking an exception to EL2, and copied to PSTATE.UAO on executing an exception return operation in EL2.	x
[22]	PAN	Privileged Access Never. Set to the value of PSTATE.PAN on taking an exception to EL2, and copied to PSTATE.PAN on executing an exception return operation in EL2.	x
[21]	SS	Software Step. Set to the value of PSTATE.SS on taking an exception to EL2, and conditionally copied to PSTATE.SS on executing an exception return operation in EL2.	x
[20]	IL	Illegal Execution state. Set to the value of PSTATE.IL on taking an exception to EL2, and copied to PSTATE.IL on executing an exception return operation in EL2.	x
[19:13]	<b>RES0</b>	Reserved	<b>RES0</b>
[12]	SSBS	Speculative Store Bypass. Set to the value of PSTATE.SSBS on taking an exception to EL2, and copied to PSTATE.SSBS on executing an exception return operation in EL2.	x
[11:10]	<b>RES0</b>	Reserved	<b>RES0</b>
[9]	D	Debug exception mask. Set to the value of PSTATE.D on taking an exception to EL2, and copied to PSTATE.D on executing an exception return operation in EL2.	x

Bits	Name	Description	Reset
[8]	A	SError interrupt mask. Set to the value of PSTATE.A on taking an exception to EL2, and copied to PSTATE.A on executing an exception return operation in EL2.	x
[7]	I	IRQ interrupt mask. Set to the value of PSTATE.I on taking an exception to EL2, and copied to PSTATE.I on executing an exception return operation in EL2.	x
[6]	F	FIQ interrupt mask. Set to the value of PSTATE.F on taking an exception to EL2, and copied to PSTATE.F on executing an exception return operation in EL2.	x
[5]	RES0	Reserved	RES0
[4]	M[4]	Execution state. Set to 0b0, the value of PSTATE.nRW, on taking an exception to EL2 from AArch64 state, and copied to PSTATE.nRW on executing an exception return operation in EL2.  <b>0b0</b> AArch64 execution state.	0b0
[3:0]	M[3:0]	AArch64 Exception level and selected Stack Pointer.  <b>0b0000</b> EL0t.  <b>0b0100</b> EL1t.  <b>0b0101</b> EL1h.  <b>0b1000</b> EL2t.  <b>0b1001</b> EL2h.  Other values are reserved. If SPSR_EL2.M[3:0] has a Reserved value, or a value for an unimplemented Exception level, executing an exception return operation in EL2 is an illegal return event, as described in <i>Illegal return events from AArch64 state</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .  The bits in this field are interpreted as follows: <ul style="list-style-type: none"> <li>M[3:2] is set to the value of PSTATE.EL on taking an exception to EL2 and copied to PSTATE.EL on executing an exception return operation in EL2.</li> <li>M[1] is unused and is 0 for all non-reserved values.</li> <li>M[0] is set to the value of PSTATE.SP on taking an exception to EL2 and copied to PSTATE.SP on executing an exception return operation in EL2.</li> </ul>	xxxx

## Access

MRS <Xt>, SPSR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0000	0b000

MSR SPSR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0000	0b000

Accessibility

MRS <Xt>, SPSR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_EL2;
```

MSR SPSR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    SPSR_EL2 = X[t, 64];
```

A.2.9.7 ELR\_EL2, Exception Link Register (EL2)

When taking an exception to EL2, holds the address to return to.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-449: AARCH64\_ELR\_EL2 bit assignments

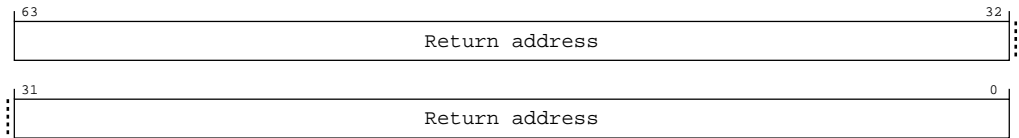


Table A-1154: ELR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Return address.  An exception return from EL2 using AArch64 makes ELR_EL2 become <b>UNKNOWN</b> .	64 {x}

Access

MRS <Xt>, ELR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0000	0b001

MSR ELR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0000	0b001

Accessibility

MRS <Xt>, ELR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = ELR_EL2;
```

MSR ELR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    ELR_EL2 = X[t, 64];
```



A.2.9.8 SP\_EL1, Stack Pointer (EL1)

Holds the stack pointer associated with EL1. When executing at EL1, the value of AArch64-SPSel.SP determines the current stack pointer:

- When AArch64-SPSel.SP == 0b0, current stack pointer is AArch64-SP\_EL0
- When AArch64-SPSel.SP == 0b1, current stack pointer is AArch64-SP\_EL1

Configurations

This register is available in all configurations.

Attributes

Width

64

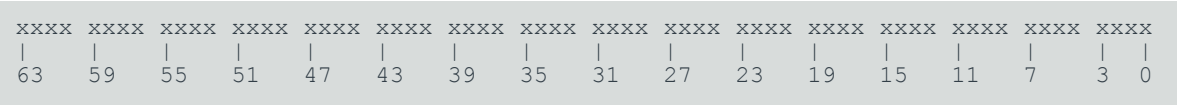
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-450: AARCH64\_SP\_EL1 bit assignments

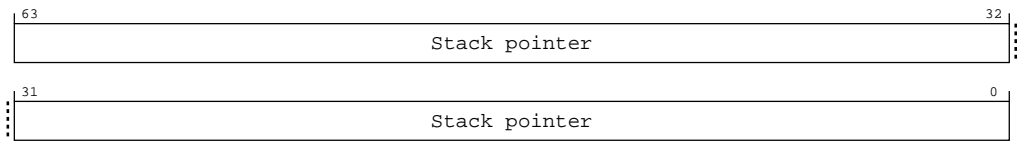


Table A-1157: SP\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Stack pointer.	64 {x}

Access

This accessibility information only applies to accesses using the MRS or MSR instructions.

When the value of AArch64-SPSel.SP is 1, this register is also accessible at EL1 as the current stack pointer.



When the value of AArch64-SPSel.SP is 0, AArch64-SP\_ELO is used as the current stack pointer at all Exception levels.

MRS <Xt>, SP\_EL1

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0001	0b000

MSR SP\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0001	0b000

Accessibility

This accessibility information only applies to accesses using the MRS or MSR instructions.

When the value of AArch64-SPSel.SP is 1, this register is also accessible at EL1 as the current stack pointer.



When the value of AArch64-SPSel.SP is 0, AArch64-SP\_ELO is used as the current stack pointer at all Exception levels.

MRS <Xt>, SP\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = SP_EL1;
```

MSR SP\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    SP_EL1 = X[t, 64];
```

A.2.9.9 SPSR\_irq, Saved Program Status Register (IRQ mode)

Holds the saved process state when an exception is taken to IRQ mode.

Configurations

This register is available in all configurations.

Attributes

Width

64

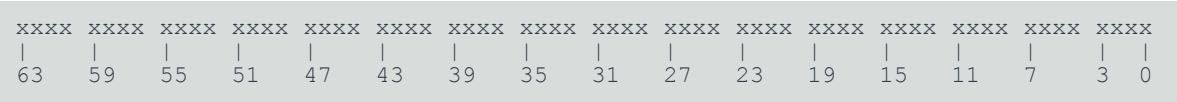
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-451: AARCH64\_SPSR\_IRQ bit assignments

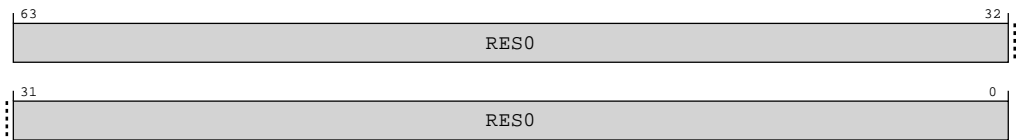


Table A-1160: SPSR\_irq bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, SPSR\_irq

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b000

MSR SPSR\_irq, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b000

Accessibility

MRS <Xt>, SPSR\_irq

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_irq;
```

MSR SPSR\_irq, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    SPSR_irq = X[t, 64];
```

A.2.9.10 SPSR\_abt, Saved Program Status Register (Abort mode)

Holds the saved process state when an exception is taken to Abort mode.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-452: AARCH64\_SPSR\_ABT bit assignments

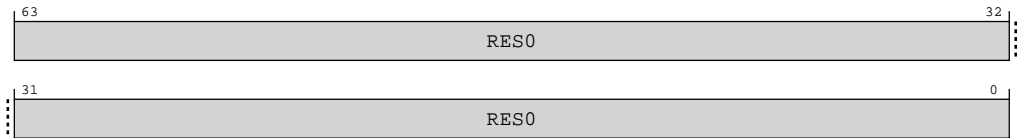


Table A-1163: SPSR\_abt bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, SPSR\_abt

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b001

MSR SPSR\_abt, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b001

Accessibility

MRS <Xt>, SPSR\_abt

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_abt;
```

MSR SPSR\_abt, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    SPSR_abt = X[t, 64];
```

A.2.9.11 SPSR\_und, Saved Program Status Register (Undefined mode)

Holds the saved process state when an exception is taken to Undefined mode.

Configurations

This register is available in all configurations.

Attributes

Width

64

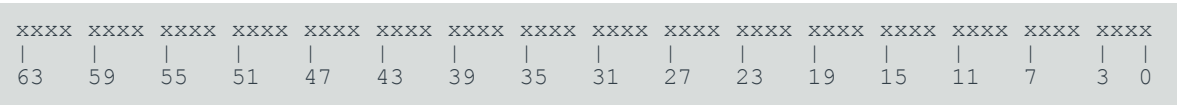
Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-453: AARCH64\_SPSR\_UND bit assignments

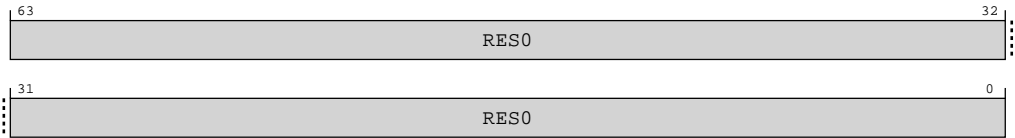


Table A-1166: SPSR\_und bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, SPSR\_und

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b010

MSR SPSR\_und, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b010

Accessibility

MRS <Xt>, SPSR\_und

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_und;
```

MSR SPSR\_und, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    SPSR_und = X[t, 64];
```

A.2.9.12 SPSR\_fiq, Saved Program Status Register (FIQ mode)

Holds the saved process state when an exception is taken to FIQ mode.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Special-purpose registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-454: AARCH64\_SPSR\_FIQ bit assignments

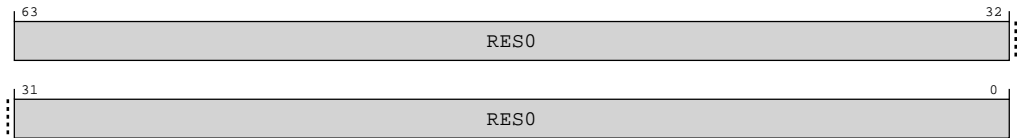


Table A-1169: SPSR\_fiq bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, SPSR\_fiq

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b011

MSR SPSR\_fiq, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0100	0b0011	0b011

Accessibility

MRS <Xt>, SPSR\_fiq

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = SPSR_fiq;
```

MSR SPSR\_fiq, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    SPSR_fiq = X[t, 64];
```



## A.2.10 AArch64 Generic Timer register description

This section includes the register descriptions for all Generic Timer registers in the Cortex®-R82AE processor.

### A.2.10.1 CNTKCTL\_EL1, Counter-timer Kernel Control Register

This register controls the generation of an event stream from the virtual counter, and access from EL0 to the physical counter, virtual counter, EL1 physical timers, and the virtual timer.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic Timer registers

##### Access type

See bit descriptions

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
0															

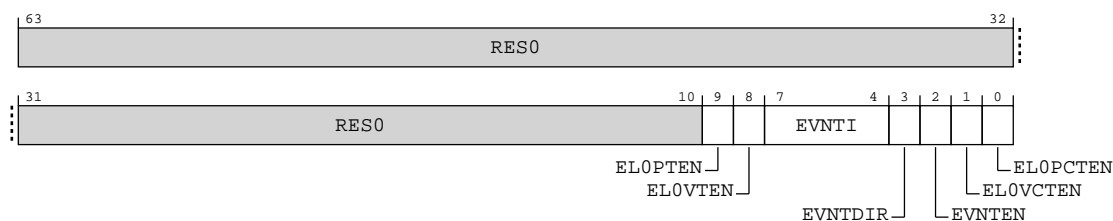


Note

Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure A-455: AARCH64\_CNTKCTL\_EL1 bit assignments



**Table A-1172: CNTKCTL\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:10]	RES0	Reserved	RES0
[9]	ELOPTEN	<p>Traps ELO accesses to the physical timer registers to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, the following registers are trapped, reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-CNTP_CTL_ELO, AArch64-CNTP_CVAL_ELO, and AArch64-CNTP_TVAL_ELO.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>ELO accesses to the physical timer registers are trapped to EL1.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[8]	ELOVTEN	<p>Traps ELO accesses to the virtual timer registers to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to the following registers are trapped, reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-CNTV_CTL_ELO, AArch64-CNTV_CVAL_ELO, and AArch64-CNTV_TVAL_ELO.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>ELO accesses to the virtual timer registers are trapped.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x
[7:4]	EVNTI	<p>Selects which bit of AArch64-CNTVCT_ELO, as seen from EL1, is the trigger for the event stream generated from that counter when that stream is enabled.</p> <p>This field selects a trigger bit in the range 0 to 15 of AArch64-CNTVCT_ELO.</p>	xxxx
[3]	EVNTDIR	<p>Controls which transition of the AArch64-CNTVCT_ELO trigger bit, as seen from EL1 and defined by EVNTI, generates an event when the event stream is enabled.</p> <p><b>0b0</b></p> <p>A 0 to 1 transition of the trigger bit triggers an event.</p> <p><b>0b1</b></p> <p>A 1 to 0 transition of the trigger bit triggers an event.</p>	x
[2]	EVNTEN	<p>Enables the generation of an event stream from AArch64-CNTVCT_ELO as seen from EL1.</p> <p><b>0b0</b></p> <p>Disables the event stream.</p> <p><b>0b1</b></p> <p>Enables the event stream.</p>	x
[1]	ELOVCTEN	<p>Traps ELO accesses to the frequency register and virtual counter register to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, as follows:</p> <ul style="list-style-type: none"> <li>In AArch64 state, accesses to the following registers are trapped and reported using EC syndrome value 0x18: <ul style="list-style-type: none"> <li>AArch64-CNTVCT_ELO and if AArch64-CNTKCTL_EL1.ELOPCTEN is 0, AArch64-CNTFRQ_ELO.</li> </ul> </li> </ul> <p><b>0b0</b></p> <p>ELO accesses to the frequency register and virtual counter registers are trapped.</p> <p><b>0b1</b></p> <p>This control does not cause any instructions to be trapped.</p>	x

Bits	Name	Description	Reset
[0]	ELOPCTEN	Traps ELO accesses to the frequency register and physical counter register to EL1, or to EL2 when it is implemented and enabled for the current Security state and AArch64-HCR_EL2.TGE is 1, as follows: <ul style="list-style-type: none"><li>In AArch64 state, the following registers are trapped, reported using EC syndrome value 0x18:<ul style="list-style-type: none"><li>AArch64-CNTPCT_ELO and if AArch64-CNTKCTL_EL1.ELOVCTEN is 0, AArch64-CNTFRQ_ELO.</li></ul></li></ul> <p><b>0b0</b></p> ELO accesses to the frequency register and physical counter register are trapped. <p><b>0b1</b></p> This control does not cause any instructions to be trapped.	x

Access

MRS <Xt>, CNTKCTL\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b11110	0b0001	0b000

MSR CNTKCTL\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b11110	0b0001	0b000

Accessibility

MRS <Xt>, CNTKCTL\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    X[t, 64] = CNTKCTL_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = CNTKCTL_EL1;
```

MSR CNTKCTL\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    CNTKCTL_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    CNTKCTL_EL1 = X[t, 64];
```

A.2.10.2 CNTFRQ\_ELO, Counter-timer Frequency Register

This register is provided so that software can discover the frequency of the system counter. It must be programmed with this value as part of system initialization. The value of the register is not interpreted by hardware.

Configurations

This register is available in all configurations.

Attributes

Width

64

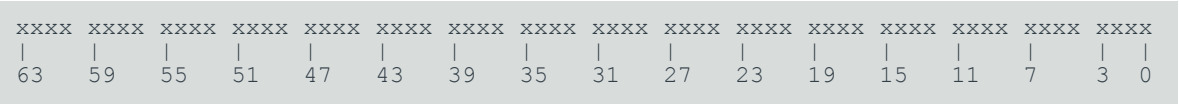
Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-456: AARCH64\_CNTFRQ\_ELO bit assignments

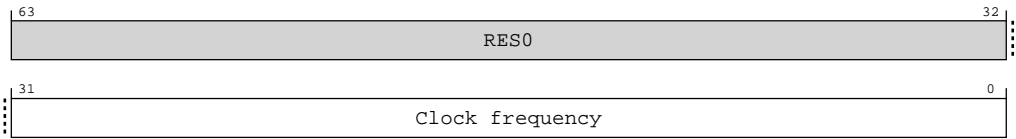


Table A-1175: CNTFRQ\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	None	Clock frequency. Indicates the system counter clock frequency, in Hz.	32 {x}

Access

MRS <Xt>, CNTFRQ\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	0b0000	0b000

MSR CNTFRQ\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	0b0000	0b000

Accessibility

MRS <Xt>, CNTFRQ\_ELO

```
if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.<EL0PCTEN,EL0VCTEN> == '00' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            X[t, 64] = CNTFRQ_ELO;
    elseif PSTATE.EL == EL1 then
        X[t, 64] = CNTFRQ_ELO;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = CNTFRQ_ELO;
```

MSR CNTFRQ\_ELO, <Xt>

```
if IsHighestEL(PSTATE.EL) then
    CNTFRQ_ELO = X[t, 64];
else
    UNDEFINED;
```

A.2.10.3 CNTPCT\_ELO, Counter-timer Physical Count Register

Holds the 64-bit physical count value.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

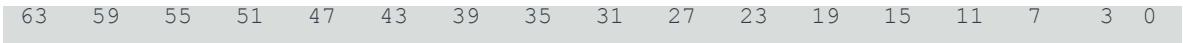
Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-457: AARCH64\_Cntpct\_El0 bit assignments

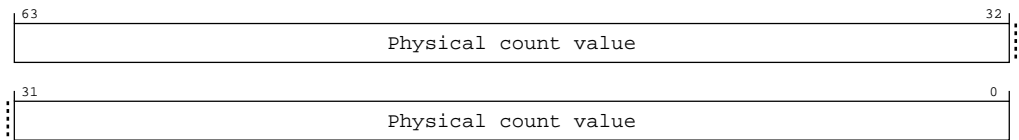


Table A-1178: Cntpct\_El0 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Physical count value.	64 {x}

Access

MRS <Xt>, Cntpct\_El0

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0000	0b001

Accessibility

MRS <Xt>, Cntpct\_El0

```
if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0PCTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elseif CNTHCTL_EL2.EL1PCTEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PhysicalCountInt();
    elseif PSTATE.EL == EL1 then
        if CNTHCTL_EL2.EL1PCTEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = PhysicalCountInt();
    elseif PSTATE.EL == EL2 then
        X[t, 64] = PhysicalCountInt();
```

A.2.10.4 CNTVCT\_EL0, Counter-timer Virtual Count Register

Holds the 64-bit virtual count value. The virtual count value is equal to the physical count value minus the virtual offset visible in AArch64-CNTVOFF\_EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

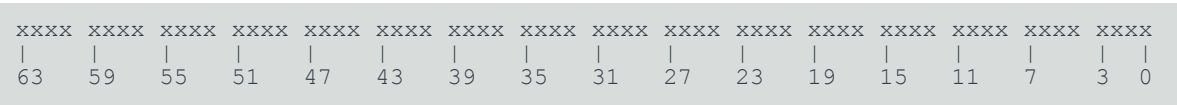
Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-458: AARCH64\_CNTVCT\_EL0 bit assignments

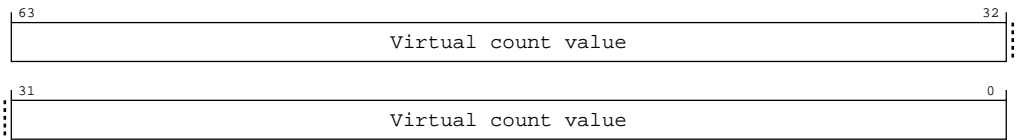


Table A-1180: CNTVCT\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Virtual count value.	64 {x}

Access

MRS <Xt>, CNTVCT\_EL0

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0000	0b010

Accessibility

MRS <Xt>, CNTVCT\_ELO

```
if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VCTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            X[t, 64] = PhysicalCountInt() - CNTVOFF_EL2;
    elseif PSTATE.EL == EL1 then
        X[t, 64] = PhysicalCountInt() - CNTVOFF_EL2;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = PhysicalCountInt() - CNTVOFF_EL2;
```

A.2.10.5 CNTP\_TVAL\_ELO, Counter-timer Physical Timer TimerValue Register

Holds the timer value for the EL1 physical timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-459: AARCH64\_CNTP\_TVAL\_ELO bit assignments

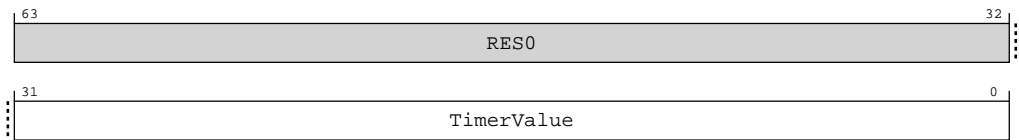


Table A-1182: CNTP\_TVAL\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	TimerValue	<p>The TimerValue view of the EL1 physical timer.</p> <p>On a read of this register:</p> <ul style="list-style-type: none"><li>If AArch64-CNTP_CTL_ELO.ENABLE is 0, the value returned is <b>UNKNOWN</b>.</li><li>If AArch64-CNTP_CTL_ELO.ENABLE is 1, the value returned is (AArch64-CNTP_CVAL_ELO - AArch64-CNTPCT_ELO).</li></ul> <p>On a write of this register, AArch64-CNTP_CVAL_ELO is set to (AArch64-CNTPCT_ELO + TimerValue), where TimerValue is treated as a signed 32-bit integer.</p> <p>When AArch64-CNTP_CTL_ELO.ENABLE is 1, the timer condition is met when (AArch64-CNTPCT_ELO - AArch64-CNTP_CVAL_ELO) is greater than or equal to zero. This means that TimerValue acts like a 32-bit downcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"><li>AArch64-CNTP_CTL_ELO.ISTATUS is set to 1.</li><li>If AArch64-CNTP_CTL_ELO.IMASK is 0, an interrupt is generated.</li></ul> <p>When AArch64-CNTP_CTL_ELO.ENABLE is 0, the timer condition is not met, but AArch64-CNTPCT_ELO continues to count, so the TimerValue view appears to continue to count down.</p> <p><b>Note:</b> The value of AArch64-CNTPCT_ELO used in these calculations is the value seen at the Exception Level that the AArch64-CNTPCT_ELO register is being read or written from.</p>	32 {x}

Access

MRS <Xt>, CNTP\_TVAL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b000

MSR CNTP\_TVAL\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b000

## Accessibility

MRS <Xt>, CNTP\_TVAL\_ELO

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0PTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif CNTHCTL_EL2.EL1PCEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            if CNTP_CTL_EL0.ENABLE == '0' then
                X[t, 64] = bits(64) UNKNOWN;
            else
                X[t, 64] = CNTP_CVAL_ELO - PhysicalCountInt();
            elsif PSTATE.EL == EL1 then
                if CNTHCTL_EL2.EL1PCEN == '0' then
                    AArch64.SystemAccessTrap(EL2, 0x18);
                else
                    if CNTP_CTL_EL0.ENABLE == '0' then
                        X[t, 64] = bits(64) UNKNOWN;
                    else
                        X[t, 64] = CNTP_CVAL_ELO - PhysicalCountInt();
            elsif PSTATE.EL == EL2 then
                if CNTP_CTL_EL0.ENABLE == '0' then
                    X[t, 64] = bits(64) UNKNOWN;
                else
                    X[t, 64] = CNTP_CVAL_ELO - PhysicalCountInt();

```

MSR CNTP\_TVAL\_ELO, <Xt>

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0PTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif CNTHCTL_EL2.EL1PCEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            CNTP_CVAL_ELO = SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt();
            elsif PSTATE.EL == EL1 then
                if CNTHCTL_EL2.EL1PCEN == '0' then
                    AArch64.SystemAccessTrap(EL2, 0x18);
                else
                    CNTP_CVAL_ELO = SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt();
            elsif PSTATE.EL == EL2 then
                CNTP_CVAL_ELO = SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt();

```

### A.2.10.6 CNTP\_CTL\_ELO, Counter-timer Physical Timer Control Register

Control register for the EL1 physical timer.

## Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-460: AARCH64\_CNTP\_CTL\_EL0 bit assignments

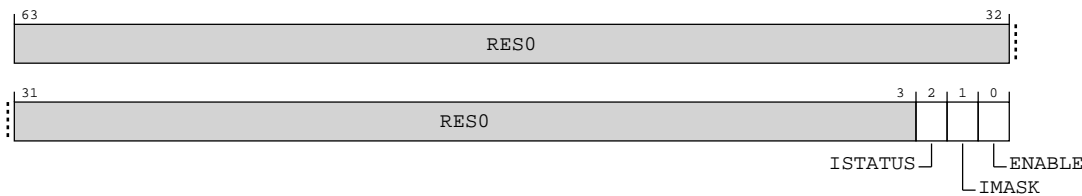


Table A-1185: CNTP\_CTL\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0
[2]	ISTATUS	<p>The status of the timer. This bit indicates whether the timer condition is met:</p> <p><b>0b0</b></p> <p>Timer condition is not met.</p> <p><b>0b1</b></p> <p>Timer condition is met.</p> <p>When the value of the ENABLE bit is 1, ISTATUS indicates whether the timer condition is met. ISTATUS takes no account of the value of the IMASK bit. If the value of ISTATUS is 1 and the value of IMASK is 0 then the timer interrupt is asserted.</p> <p>When the value of the ENABLE bit is 0, the ISTATUS field is <b>UNKNOWN</b>.</p> <p>Access to this field is: RO</p>	x

Bits	Name	Description	Reset
[1]	IMASK	<p>Timer interrupt mask bit. Permitted values are:</p> <p><b>0b0</b> Timer interrupt is not masked by the IMASK bit.</p> <p><b>0b1</b> Timer interrupt is masked by the IMASK bit.</p> <p>For more information, see the description of the ISTATUS bit.</p>	x
[0]	ENABLE	<p>Enables the timer. Permitted values are:</p> <p><b>0b0</b> Timer disabled.</p> <p><b>0b1</b> Timer enabled.</p> <p>Setting this bit to 0 disables the timer output signal, but the timer value accessible from AArch64-CNTP_TVAL_ELO continues to count down.</p> <p><b>Note:</b> Disabling the output signal might be a power-saving option.</p>	x

## Access

MRS <Xt>, CNTP\_CTL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b001

MSR CNTP\_CTL\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b001

## Accessibility

MRS <Xt>, CNTP\_CTL\_ELO

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0PTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        elsif CNTHCTL_EL2.EL1PCEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = CNTP_CTL_ELO;
    elsif PSTATE.EL == EL1 then
        if CNTHCTL_EL2.EL1PCEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = CNTP_CTL_ELO;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = CNTP_CTL_ELO;

```

MSR CNTP\_CTL\_EL0, <Xt>

```
if PSTATE.EL == EL0 then
  if CNTKCTL_EL1.EL0PTEN == '0' then
    if HCR_EL2.TGE == '1' then
      AArch64.SystemAccessTrap(EL2, 0x18);
    else
      AArch64.SystemAccessTrap(EL1, 0x18);
  elseif CNTHCTL_EL2.EL1PCEN == '0' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    CNTP_CTL_EL0 = X[t, 64];
elseif PSTATE.EL == EL1 then
  if CNTHCTL_EL2.EL1PCEN == '0' then
    AArch64.SystemAccessTrap(EL2, 0x18);
  else
    CNTP_CTL_EL0 = X[t, 64];
elseif PSTATE.EL == EL2 then
  CNTP_CTL_EL0 = X[t, 64];
```

A.2.10.7 CNTP\_CVAL\_EL0, Counter-timer Physical Timer CompareValue Register

Holds the compare value for the EL1 physical timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-461: AARCH64\_CNTP\_CVAL\_ELO bit assignments

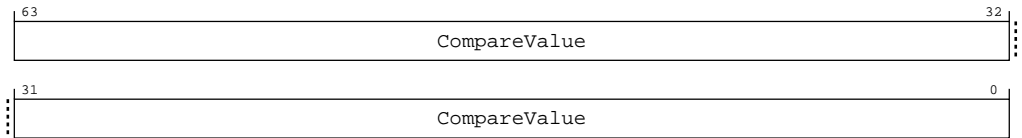


Table A-1188: CNTP\_CVAL\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	CompareValue	<p>Holds the EL1 physical timer CompareValue.</p> <p>When AArch64-CNTP_CTL_ELO.ENABLE is 1, the timer condition is met when (AArch64-CNTPCT_ELO - CompareValue) is greater than or equal to zero. This means that CompareValue acts like a 64-bit upcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"><li>AArch64-CNTP_CTL_ELO.ISTATUS is set to 1.</li><li>If AArch64-CNTP_CTL_ELO.IMASK is 0, an interrupt is generated.</li></ul> <p>When AArch64-CNTP_CTL_ELO.ENABLE is 0, the timer condition is not met, but AArch64-CNTPCT_ELO continues to count.</p> <p>If the Generic counter is implemented at a size less than 64 bits, then this field is permitted to be implemented at the same width as the counter, and the upper bits are <b>RESO</b>.</p> <p>The value of this field is treated as zero-extended in all counter calculations.</p>	64 {x}

Access

MRS <Xt>, CNTP\_CVAL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b010

MSR CNTP\_CVAL\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0010	0b010

Accessibility

MRS <Xt>, CNTP\_CVAL\_ELO

```
if PSTATE.EL == EL0 then
  if CNTKCTL_EL1.EL0PTEN == '0' then
    if HCR_EL2.TGE == '1' then
      AArch64.SystemAccessTrap(EL2, 0x18);
    else
      AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CNTHCTL_EL2.EL1PCEN == '0' then
      AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

```
        X[t, 64] = CNTP_CVAL_EL0;
    elseif PSTATE.EL == EL1 then
        if CNTHCTL_EL2.EL1PCEN == '0' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = CNTP_CVAL_EL0;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = CNTP_CVAL_EL0;
```

MSR CNTP\_CVAL\_EL0, <Xt>

```
if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0PTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
    elseif CNTHCTL_EL2.EL1PCEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        CNTP_CVAL_EL0 = X[t, 64];
elseif PSTATE.EL == EL1 then
    if CNTHCTL_EL2.EL1PCEN == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        CNTP_CVAL_EL0 = X[t, 64];
elseif PSTATE.EL == EL2 then
    CNTP_CVAL_EL0 = X[t, 64];
```

A.2.10.8 CNTV\_TVAL\_EL0, Counter-timer Virtual Timer TimerValue Register

Holds the timer value for the EL1 virtual timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-462: AARCH64\_CNTV\_TVAL\_ELO bit assignments

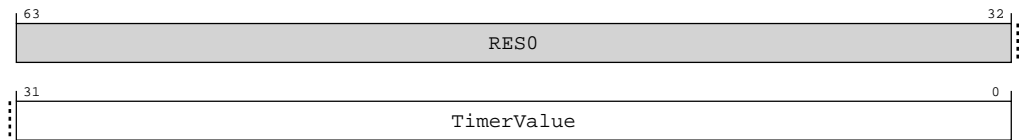


Table A-1191: CNTV\_TVAL\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	TimerValue	<p>The TimerValue view of the EL1 virtual timer.</p> <p>On a read of this register:</p> <ul style="list-style-type: none"><li>If AArch64-CNTV_CTL_ELO.ENABLE is 0, the value returned is <b>UNKNOWN</b>.</li><li>If AArch64-CNTV_CTL_ELO.ENABLE is 1, the value returned is (AArch64-CNTV_CVAL_ELO - AArch64-CNTVCT_ELO).</li></ul> <p>On a write of this register, AArch64-CNTV_CVAL_ELO is set to (AArch64-CNTVCT_ELO + TimerValue), where TimerValue is treated as a signed 32-bit integer.</p> <p>When AArch64-CNTV_CTL_ELO.ENABLE is 1, the timer condition is met when (AArch64-CNTVCT_ELO - AArch64-CNTV_CVAL_ELO) is greater than or equal to zero. This means that TimerValue acts like a 32-bit downcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"><li>AArch64-CNTV_CTL_ELO.ISTATUS is set to 1.</li><li>If AArch64-CNTV_CTL_ELO.IMASK is 0, an interrupt is generated.</li></ul> <p>When AArch64-CNTV_CTL_ELO.ENABLE is 0, the timer condition is not met, but AArch64-CNTVCT_ELO continues to count, so the TimerValue view appears to continue to count down.</p>	32 {x}

Access

MRS <Xt>, CNTV\_TVAL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0011	0b000

MSR CNTV\_TVAL\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0011	0b000



## Accessibility

MRS <Xt>, CNTV\_TVAL\_ELO

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            if CNTV_CTL_EL0.ENABLE == '0' then
                X[t, 64] = bits(64) UNKNOWN;
            else
                X[t, 64] = CNTV_CVAL_ELO - (PhysicalCountInt() - CNTVOFF_EL2);
    elseif PSTATE.EL == EL1 then
        if CNTV_CTL_EL0.ENABLE == '0' then
            X[t, 64] = bits(64) UNKNOWN;
        else
            X[t, 64] = CNTV_CVAL_ELO - (PhysicalCountInt() - CNTVOFF_EL2);
    elseif PSTATE.EL == EL2 then
        if CNTV_CTL_EL0.ENABLE == '0' then
            X[t, 64] = bits(64) UNKNOWN;
        else
            X[t, 64] = CNTV_CVAL_ELO - (PhysicalCountInt() - CNTVOFF_EL2);

```

MSR CNTV\_TVAL\_ELO, <Xt>

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            CNTV_CVAL_ELO = (SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt()) -
                CNTVOFF_EL2;
    elseif PSTATE.EL == EL1 then
        CNTV_CVAL_ELO = (SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt()) -
            CNTVOFF_EL2;
    elseif PSTATE.EL == EL2 then
        CNTV_CVAL_ELO = (SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt()) -
            CNTVOFF_EL2;

```

### A.2.10.9 CNTV\_CTL\_ELO, Counter-timer Virtual Timer Control Register

Control register for the virtual timer.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

64

##### Functional group

Generic Timer registers

Access type  
RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-463: AARCH64\_CNTV\_CTL\_EL0 bit assignments

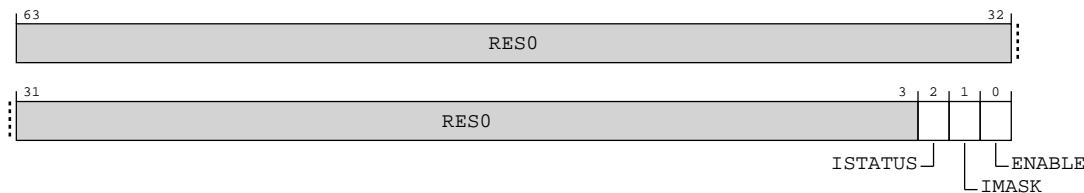


Table A-1194: CNTV\_CTL\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0
[2]	ISTATUS	<p>The status of the timer. This bit indicates whether the timer condition is met:</p> <p><b>0b0</b></p> <p>Timer condition is not met.</p> <p><b>0b1</b></p> <p>Timer condition is met.</p> <p>When the value of the ENABLE bit is 1, ISTATUS indicates whether the timer condition is met. ISTATUS takes no account of the value of the IMASK bit. If the value of ISTATUS is 1 and the value of IMASK is 0 then the timer interrupt is asserted.</p> <p>When the value of the ENABLE bit is 0, the ISTATUS field is <b>UNKNOWN</b>.</p> <p>Access to this field is: RO</p>	x
[1]	IMASK	<p>Timer interrupt mask bit. Permitted values are:</p> <p><b>0b0</b></p> <p>Timer interrupt is not masked by the IMASK bit.</p> <p><b>0b1</b></p> <p>Timer interrupt is masked by the IMASK bit.</p> <p>For more information, see the description of the ISTATUS bit.</p>	x

Bits	Name	Description	Reset
[0]	ENABLE	<p>Enables the timer. Permitted values are:</p> <p><b>0b0</b> Timer disabled.</p> <p><b>0b1</b> Timer enabled.</p> <p>Setting this bit to 0 disables the timer output signal, but the timer value accessible from AArch64-CNTV_TVAL_ELO continues to count down.</p> <p><b>Note:</b> Disabling the output signal might be a power-saving option.</p>	x

### Access

MRS <Xt>, CNTV\_CTL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	0b0011	0b001

MSR CNTV\_CTL\_ELO, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b011	0b11110	0b0011	0b001

### Accessibility

MRS <Xt>, CNTV\_CTL\_ELO

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            X[t, 64] = CNTV_CTL_ELO;
    elseif PSTATE.EL == EL1 then
        X[t, 64] = CNTV_CTL_ELO;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = CNTV_CTL_ELO;

```

MSR CNTV\_CTL\_ELO, <Xt>

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            CNTV_CTL_ELO = X[t, 64];
    elseif PSTATE.EL == EL1 then
        CNTV_CTL_ELO = X[t, 64];

```

```
elseif PSTATE.EL == EL2 then
    CNTV_CTL_EL0 = X[t, 64];
```

A.2.10.10 CNTV\_CVAL\_EL0, Counter-timer Virtual Timer CompareValue Register

Holds the compare value for the virtual timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

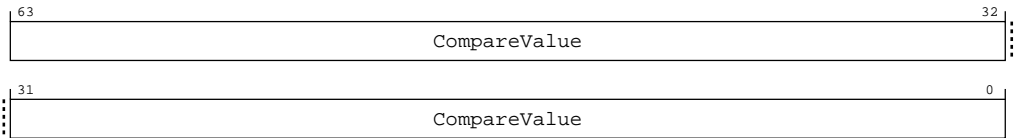
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-464: AARCH64\_CNTV\_CVAL\_EL0 bit assignments



**Table A-1197: CNTV\_CVAL\_ELO bit descriptions**

Bits	Name	Description	Reset
[63:0]	CompareValue	<p>Holds the EL1 virtual timer CompareValue.</p> <p>When AArch64-CNTV_CTL_ELO.ENABLE is 1, the timer condition is met when (AArch64-CNTVCT_ELO - CompareValue) is greater than or equal to zero. This means that CompareValue acts like a 64-bit upcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"> <li>AArch64-CNTV_CTL_ELO.ISTATUS is set to 1.</li> <li>If AArch64-CNTV_CTL_ELO.IMASK is 0, an interrupt is generated.</li> </ul> <p>When AArch64-CNTV_CTL_ELO.ENABLE is 0, the timer condition is not met, but AArch64-CNTVCT_ELO continues to count.</p> <p>If the Generic counter is implemented at a size less than 64 bits, then this field is permitted to be implemented at the same width as the counter, and the upper bits are <b>RES0</b>.</p> <p>The value of this field is treated as zero-extended in all counter calculations.</p>	64 {x}

### Access

MRS &lt;Xt&gt;, CNTV\_CVAL\_ELO

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0011	0b010

MSR CNTV\_CVAL\_ELO, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b011	0b1110	0b0011	0b010

### Accessibility

MRS &lt;Xt&gt;, CNTV\_CVAL\_ELO

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);
        else
            X[t, 64] = CNTV_CVAL_ELO;
    elseif PSTATE.EL == EL1 then
        X[t, 64] = CNTV_CVAL_ELO;
    elseif PSTATE.EL == EL2 then
        X[t, 64] = CNTV_CVAL_ELO;

```

MSR CNTV\_CVAL\_ELO, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    if CNTKCTL_EL1.EL0VTEN == '0' then
        if HCR_EL2.TGE == '1' then
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            AArch64.SystemAccessTrap(EL1, 0x18);

```

```
else
    CNTV_CVAL_EL0 = X[t, 64];
elseif PSTATE.EL == EL1 then
    CNTV_CVAL_EL0 = X[t, 64];
elseif PSTATE.EL == EL2 then
    CNTV_CVAL_EL0 = X[t, 64];
```

A.2.10.11 CNTVOFF\_EL2, Counter-timer Virtual Offset Register

Holds the 64-bit virtual offset. This is the offset between the physical count value visible in AArch64-CNTPCT\_ELO and the virtual count value visible in AArch64-CNTVCT\_ELO.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

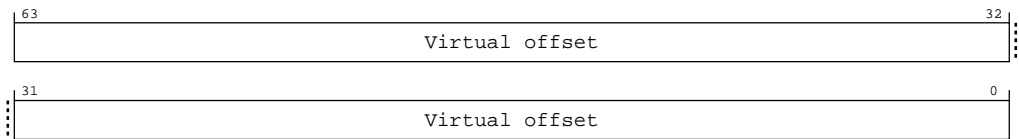
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-465: AARCH64\_CNTVOFF\_EL2 bit assignments



**Table A-1200: CNTVOFF\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:0]	None	Virtual offset.  If the Generic counter is implemented at a size less than 64 bits, then this field is permitted to be implemented at the same width as the counter, and the upper bits are <b>RES0</b> .  The value of this field is treated as zero-extended in all counter calculations.	64 {x}

**Access**

MRS &lt;Xt&gt;, CNTVOFF\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1110	0b0000	0b011

MSR CNTVOFF\_EL2, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b100	0b1110	0b0000	0b011

**Accessibility**

MRS &lt;Xt&gt;, CNTVOFF\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = CNTVOFF_EL2;

```

MSR CNTVOFF\_EL2, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    CNTVOFF_EL2 = X[t, 64];

```

**A.2.10.12 CNTHCTL\_EL2, Counter-timer Hypervisor Control Register**

Controls the generation of an event stream from the physical counter, and access from EL1 to the physical counter and the EL1 physical timer.

**Configurations**

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

The following field descriptions apply in all Armv8.0 implementations.

Figure A-466: AARCH64\_CNTHCTL\_EL2 bit assignments

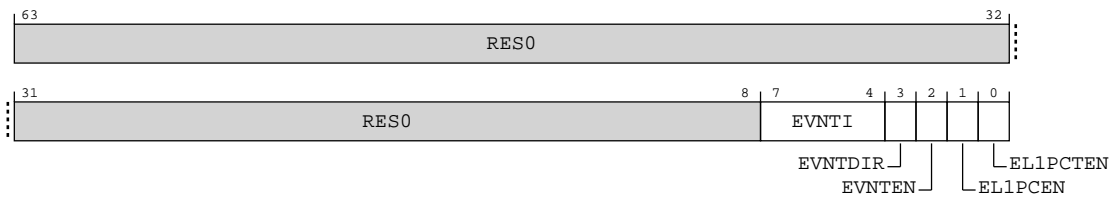


Table A-1203: CNTHCTL\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:4]	EVNTI	Selects which bit of AArch64-CNTPCT_ELO, as seen from EL2,is the trigger for the event stream generated from that counter when that stream is enabled.  This field selects a trigger bit in the range 0 to 15 of AArch64-CNTPCT_ELO.	xxxx
[3]	EVNTDIR	Controls which transition of the AArch64-CNTPCT_ELO trigger bit, as seen from EL2 and defined by EVNTI, generates an event when the event stream is enabled.  <b>0b0</b> A 0 to 1 transition of the trigger bit triggers an event.  <b>0b1</b> A 1 to 0 transition of the trigger bit triggers an event.	x



Bits	Name	Description	Reset
[2]	EVNTEN	Enables the generation of an event stream from AArch64-CNTPCT_ELO as seen from EL2.  <b>0b0</b> Disables the event stream.  <b>0b1</b> Enables the event stream.	x
[1]	EL1PCEN	Traps ELO and EL1 accesses to the EL1 physical timer registers to EL2 when EL2 is enabled in the current Security state, as follows: <ul style="list-style-type: none"> <li>In AArch64 state, accesses to AArch64-CNTP_CTL_ELO, AArch64-CNTP_CVAL_ELO, AArch64-CNTP_TVAL_ELO are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <b>0b0</b> From AArch64 state: ELO and EL1 accesses to the AArch64-CNTP_CTL_ELO, AArch64-CNTP_CVAL_ELO, and AArch64-CNTP_TVAL_ELO are trapped to EL2 when EL2 is enabled in the current Security state, unless they are trapped by AArch64-CNTKCTL_EL1.ELOPTEN.  <b>0b1</b> This control does not cause any instructions to be trapped.	x
[0]	EL1PCTEN	Traps ELO and EL1 accesses to the EL1 physical counter register to EL2 when EL2 is enabled in the current Security state, as follows: <ul style="list-style-type: none"> <li>In AArch64 state, accesses to AArch64-CNTPCT_ELO are trapped to EL2, reported using EC syndrome value 0x18.</li> </ul> <b>0b0</b> From AArch64 state: ELO and EL1 accesses to the AArch64-CNTPCT_ELO are trapped to EL2 when EL2 is enabled in the current Security state, unless they are trapped by AArch64-CNTKCTL_EL1.ELOPCTEN.  <b>0b1</b> This control does not cause any instructions to be trapped.	x

## Access

MRS <Xt>, CNTHCTL\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0001	0b000

MSR CNTHCTL\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0001	0b000

## Accessibility

MRS <Xt>, CNTHCTL\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CNTHCTL_EL2;

```

MSR CNTHCTL\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    CNTHCTL_EL2 = X[t, 64];
```

A.2.10.13 CNTHPS\_TVAL\_EL2, Counter-timer Secure Physical Timer TimerValue Register (EL2)

Holds the timer value for the Secure EL2 physical timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0

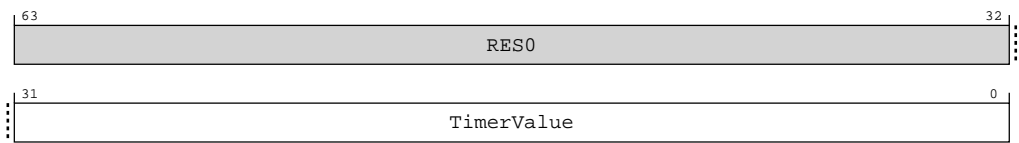


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-467: AARCH64\_CNTHPS\_TVAL\_EL2 bit assignments



**Table A-1206: CNTHPS\_TVAL\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	TimerValue	<p>The TimerValue view of the EL2 physical timer.</p> <p>On a read of this register:</p> <ul style="list-style-type: none"> <li>If AArch64-CNTHPS_CTL_EL2.ENABLE is 0, the value returned is <b>UNKNOWN</b>.</li> <li>If AArch64-CNTHPS_CTL_EL2.ENABLE is 1, the value returned is (AArch64-CNTHPS_CVAL_EL2 - AArch64-CNTPCT_ELO).</li> </ul> <p>On a write of this register, AArch64-CNTHPS_CVAL_EL2 is set to (AArch64-CNTPCT_ELO + TimerValue), where TimerValue is treated as a signed 32-bit integer.</p> <p>When AArch64-CNTHPS_CTL_EL2.ENABLE is 1, the timer condition is met when (AArch64-CNTPCT_ELO - AArch64-CNTHPS_CVAL_EL2) is greater than or equal to zero. This means that TimerValue acts like a 32-bit downcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"> <li>AArch64-CNTHPS_CTL_EL2.ISTATUS is set to 1.</li> <li>If AArch64-CNTHPS_CTL_EL2.IMASK is 0, an interrupt is generated.</li> </ul> <p>When AArch64-CNTHPS_CTL_EL2.ENABLE is 0, the timer condition is not met, but AArch64-CNTPCT_ELO continues to count, so the TimerValue view appears to continue to count down.</p>	32 {x}

### Access

MRS &lt;Xt&gt;, CNTHPS\_TVAL\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0101	0b000

MSR CNTHPS\_TVAL\_EL2, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0101	0b000

### Accessibility

MRS &lt;Xt&gt;, CNTHPS\_TVAL\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    if CNTHPS_CTL_EL2.ENABLE == '0' then
        X[t, 64] = bits(64) UNKNOWN;
    else
        X[t, 64] = CNTHPS_CVAL_EL2 - PhysicalCountInt();

```

MSR CNTHPS\_TVAL\_EL2, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then

```

```
    UNDEFINED;
    elsif PSTATE.EL == EL2 then
        CNTHPS_CVAL_EL2 = SignExtend(X[t, 64]<31:0>, 64) + PhysicalCountInt();
```

A.2.10.14 CNTHPS\_CTL\_EL2, Counter-timer Secure Physical Timer Control Register (EL2)

Control register for the Secure EL2 physical timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

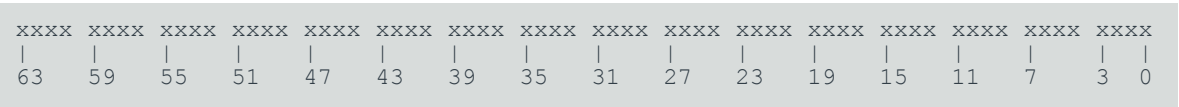
Functional group

Generic Timer registers

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-468: AARCH64\_CNTHPS\_CTL\_EL2 bit assignments

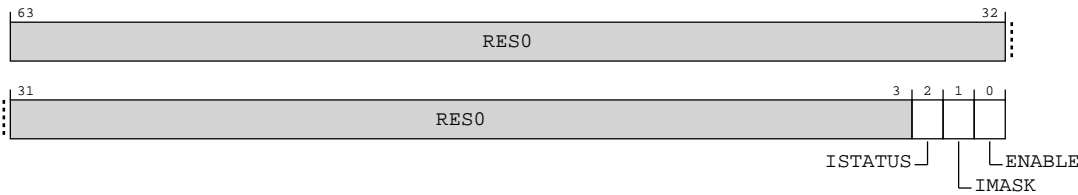


Table A-1209: CNTHPS\_CTL\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2]	ISTATUS	<p>The status of the timer. This bit indicates whether the timer condition is met:</p> <p><b>0b0</b> Timer condition is not met.</p> <p><b>0b1</b> Timer condition is met.</p> <p>When the value of the CNTHPS_CTL_EL2.ENABLE bit is 1, ISTATUS indicates whether the timer condition is met. ISTATUS takes no account of the value of the IMASK bit. If the value of ISTATUS is 1 and the value of IMASK is 0 then the timer interrupt is asserted.</p> <p>When the value of the CNTHPS_CTL_EL2.ENABLE bit is 0, the ISTATUS field is <b>UNKNOWN</b>.</p> <p>Access to this field is: RO</p>	x
[1]	IMASK	<p>Timer interrupt mask bit. Permitted values are:</p> <p><b>0b0</b> Timer interrupt is not masked by the IMASK bit.</p> <p><b>0b1</b> Timer interrupt is masked by the IMASK bit.</p> <p>For more information, see the description of the ISTATUS bit.</p>	x
[0]	ENABLE	<p>Enables the timer. Permitted values are:</p> <p><b>0b0</b> Timer disabled.</p> <p><b>0b1</b> Timer enabled.</p> <p>Setting this bit to 0 disables the timer output signal, but the timer value accessible from AArch64-CNTHPS_TVAL_EL2 continues to count down.</p> <p><b>Note:</b> Disabling the output signal might be a power-saving option.</p>	x

## Access

MRS <Xt>, CNTHPS\_CTL\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1110	0b0101	0b001

MSR CNTHPS\_CTL\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1110	0b0101	0b001

Accessibility

MRS <Xt>, CNTHPS\_CTL\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CNTHPS_CTL_EL2;
```

MSR CNTHPS\_CTL\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    CNTHPS_CTL_EL2 = X[t, 64];
```

A.2.10.15 CNTHPS\_CVAL\_EL2, Counter-timer Secure Physical Timer CompareValue Register (EL2)

Holds the compare value for the Secure EL2 physical timer.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Generic Timer registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-469: AARCH64\_CNTHPS\_CVAL\_EL2 bit assignments

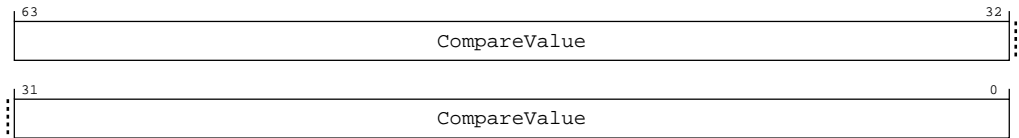


Table A-1212: CNTHPS\_CVAL\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	CompareValue	<p>Holds the EL2 physical timer CompareValue.</p> <p>When AArch64-CNTHPS_CTL_EL2.ENABLE is 1, the timer condition is met when (AArch64-CNTPCT_ELO - CompareValue) is greater than or equal to zero. This means that CompareValue acts like a 64-bit upcounter timer. When the timer condition is met:</p> <ul style="list-style-type: none"><li>AArch64-CNTHPS_CTL_EL2.ISTATUS is set to 1.</li><li>If AArch64-CNTHPS_CTL_EL2.IMASK is 0, an interrupt is generated.</li></ul> <p>When AArch64-CNTHPS_CTL_EL2.ENABLE is 0, the timer condition is not met, but AArch64-CNTPCT_ELO continues to count.</p> <p>If the Generic counter is implemented at a size less than 64 bits, then this field is permitted to be implemented at the same width as the counter, and the upper bits are <b>RESO</b>.</p> <p>The value of this field is treated as zero-extended in all counter calculations.</p>	64 {x}

Access

MRS <Xt>, CNTHPS\_CVAL\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0101	0b010

MSR CNTHPS\_CVAL\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b11110	0b0101	0b010

Accessibility

MRS <Xt>, CNTHPS\_CVAL\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = CNTHPS_CVAL_EL2;
```

MSR CNTHPS\_CVAL\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    CNTHPS_CVAL_EL2 = X[t, 64];
```

A.2.11 AArch64 other register description

This section includes the register descriptions for all other registers in the Cortex®-R82AE processor.

A.2.11.1 IMP\_TESTRO\_EL1, STL Test Register 0

This register provides read-only, **IMPLEMENTATION DEFINED** testing functionality for the core.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure A-470: AARCH64\_IMP\_TESTRO\_EL1 bit assignments

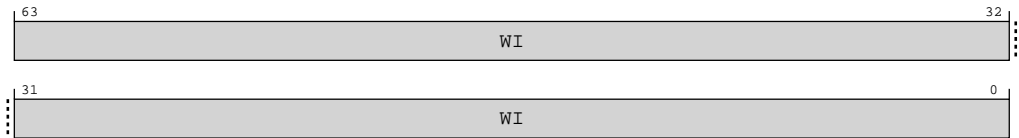


Table A-1215: IMP\_TESTRO\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	WI	Reserved	WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ**.

MRS <Xt>, IMP\_TESTRO\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b001

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ.

MRS <Xt>, IMP\_TESTRO\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_TESTRO_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_TESTRO_EL1;
```

A.2.11.2 IMP\_TESTR1\_EL1, STL Test Register 1

This register provides **IMPLEMENTATION DEFINED** testing functionality for the core.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-471: AARCH64\_IMP\_TESTR1\_EL1 bit assignments

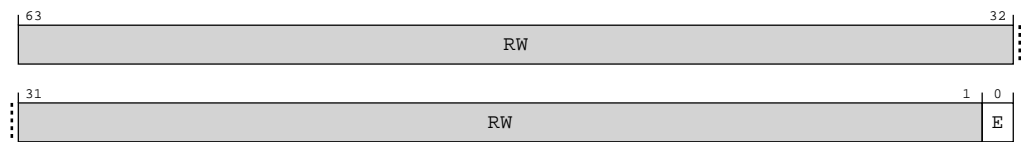


Table A-1217: IMP\_TESTR1\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:1]	RW	Reserved	RW
[0]	E	Enable.  <b>0b0</b>  Any core control options affected by IMP_TESTR1_EL1 are disabled.  <b>0b1</b>  <b>IMPLEMENTATION DEFINED</b> core control options enabled. Arm strongly recommends that you do not set this field to 0b1 unless directed by Arm.	0b0

Access

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_TESTR1\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b010

MSR IMP\_TESTR1\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b010

### Accessibility

Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_TESTR1\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_TESTR1_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_TESTR1_EL1;

```

MSR IMP\_TESTR1\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.TESTR1 == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_TESTR1_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_TESTR1_EL1 = X[t, 64];

```

### A.2.11.3 IMP\_TESTR1KEY\_EL1, STL TESTR1 Write Key Register

Key register to enable AArch64-IMP\_TESTR1\_EL1 and AArch64-IMP\_TESTR2\_EL1 writes. Software must write a specific value to this register before subsequent writes to AArch64-IMP\_TESTR1\_EL1 or AArch64-IMP\_TESTR2\_EL1, otherwise the writes to AArch64-IMP\_TESTR1\_EL1 or AArch64-IMP\_TESTR2\_EL1 are ignored.

This register is reserved for the STL use. Arm strongly recommends that you do not modify this register unless directed by Arm.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

64

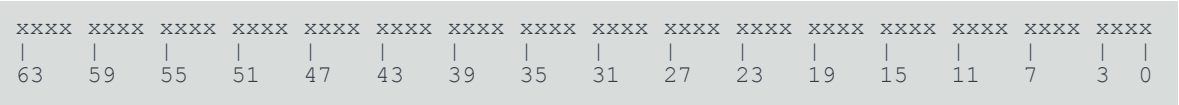
#### Functional group

Other system control registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-472: AARCH64\_IMP\_TESTR1KEY\_EL1 bit assignments

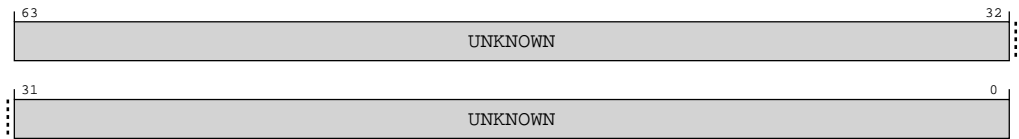


Table A-1220: IMP\_TESTR1KEY\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.  
[ ote]

MSR IMP\_TESTR1KEY\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b011

Accessibility



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.  
[ ote]

MSR IMP\_TESTR1KEY\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.TESTR1 == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_TESTR1KEY_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_TESTR1KEY_EL1 = X[t, 64];
```

A.2.11.4 IMP\_LFSR\_EL1, STL LFSR Pseudo-random Value Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-473: AARCH64\_IMP\_LFSR\_EL1 bit assignments

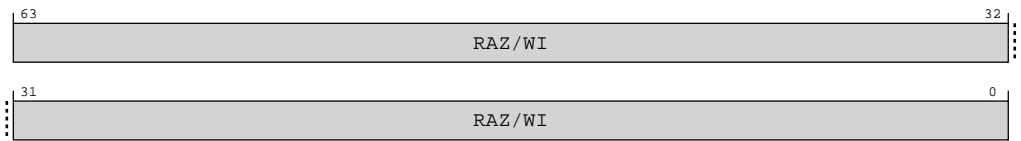


Table A-1222: IMP\_LFSR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_LFSR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b100

MSR IMP\_LFSR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b0010	0b100

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_LFSR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_LFSR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_LFSR_EL1;
```

MSR IMP\_LFSR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_LFSR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_LFSR_EL1 = X[t, 64];
```

A.2.11.5 IMP\_FCTLR\_EL1, Fault Control Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-474: AARCH64\_IMP\_FCTLR\_EL1 bit assignments

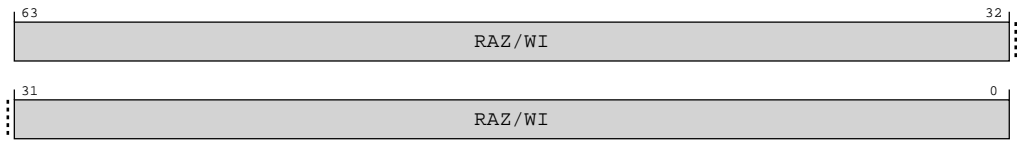


Table A-1225: IMP\_FCTLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Note

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FCTLR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b000

MSR IMP\_FCTLR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b000

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FCTLR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_FCTLR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_FCTLR_EL1;
```

MSR IMP\_FCTLR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_FCTLR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_FCTLR_EL1 = X[t, 64];
```

A.2.11.6 IMP\_FPIR\_EL1, Fault Partition Identifier Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is available in all configurations.



Attributes

Width  
64

Functional group  
Other system control registers

Access type  
See bit descriptions

Reset value  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-475: AARCH64\_IMP\_FPIR\_EL1 bit assignments

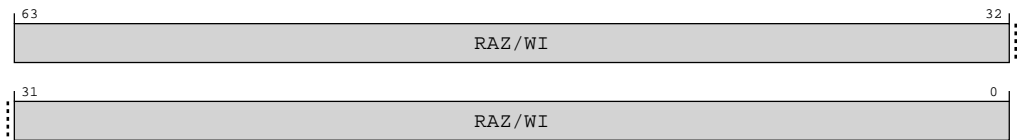


Table A-1228: IMP\_FPIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FPIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b001

MSR IMP\_FPIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b001

## Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FPIR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_FPIR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_FPIR_EL1;

```

MSR IMP\_FPIR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_FPIR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_FPIR_EL1 = X[t, 64];

```

### A.2.11.7 IMP\_FFMIR\_EL1, Fault Failure Mode Identification Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

## Configurations

This register is available in all configurations.

## Attributes

### Width

64

### Functional group

Other system control registers

### Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-476: AARCH64\_IMP\_FFMIR\_EL1 bit assignments

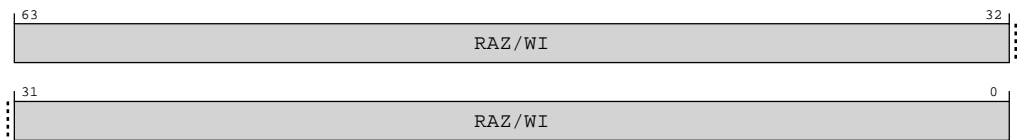


Table A-1231: IMP\_FFMIR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FFMIR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b010

MSR IMP\_FFMIR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b010

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_FFMIR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_FFMIR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_FFMIR_EL1;
```

MSR IMP\_FFMIR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_FFMIR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_FFMIR_EL1 = X[t, 64];
```

A.2.11.8 IMP\_TESTR2\_EL1, STL Test Register 2

This register enables easier testing with the Software Test Library, by making some parts of the CPU hardware status to be observable.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-477: AARCH64\_IMP\_TESTR2\_EL1 bit assignments

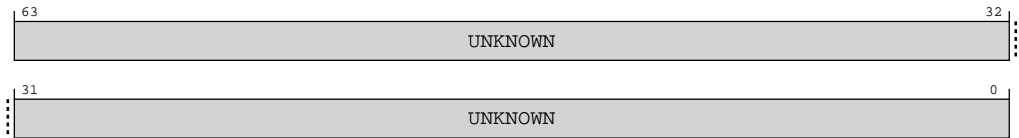


Table A-1234: IMP\_TESTR2\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	UNKNOWN	Reserved	UNKNOWN

Access

Software must write a specific value to AArch64-IMP\_TESTR1KEY\_EL1 before subsequent writes to AArch64-IMP\_TESTR2\_EL1, otherwise the writes to AArch64-IMP\_TESTR2\_EL1 are ignored.

MRS <Xt>, IMP\_TESTR2\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b100

MSR IMP\_TESTR2\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1000	0b100

Accessibility

Software must write a specific value to AArch64-IMP\_TESTR1KEY\_EL1 before subsequent writes to AArch64-IMP\_TESTR2\_EL1, otherwise the writes to AArch64-IMP\_TESTR2\_EL1 are ignored.

MRS <Xt>, IMP\_TESTR2\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_TESTR2_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_TESTR2_EL1;
```

MSR IMP\_TESTR2\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' || ACTLR_EL2.TESTR1 == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
```

```
IMP_TESTR2_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_TESTR2_EL1 = X[t, 64];
```

A.2.11.9 IMP\_PMCCTRL\_EL1, STL Main Control Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCCTRL\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000 0000  
  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000 0000  
  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000 0000

Bit descriptions

Figure A-478: AARCH64\_IMP\_PMCCTRL\_EL1 bit assignments

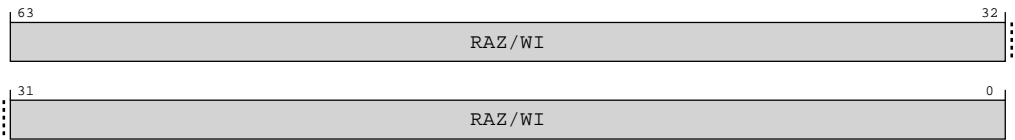


Table A-1237: IMP\_PMCCTRL\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCCTRL\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b000

MSR IMP\_PMCCTRL\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b000

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCCTRL\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCCTRL_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCCTRL_EL1;
```

MSR IMP\_PMCCTRL\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCCTRL_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCCTRL_EL1 = X[t, 64];
```

A.2.11.10 IMP\_PMC MCR\_EL1, STL Memory Control Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMC MCR\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-479: AARCH64\_IMP\_PMC MCR\_EL1 bit assignments

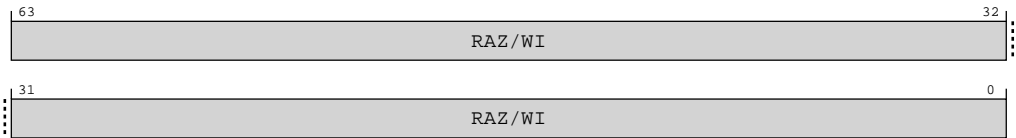



Table A-1240: IMP\_PMC MCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Note

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMC MCR\_EL1



op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b001

MSR IMP\_PMCPCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b001

## Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCPCR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCPCR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_PMCPCR_EL1;
```

MSR IMP\_PMCPCR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCPCR_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_PMCPCR_EL1 = X[t, 64];
```

### A.2.11.11 IMP\_PMCBER\_EL1, STL Byte Enable Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

## Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCBER\_EL1 are UNDEFINED.

Attributes

Width  
64

Functional group  
Other system control registers

Access type  
See bit descriptions

Reset value  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-480: AARCH64\_IMP\_PMCBER\_EL1 bit assignments

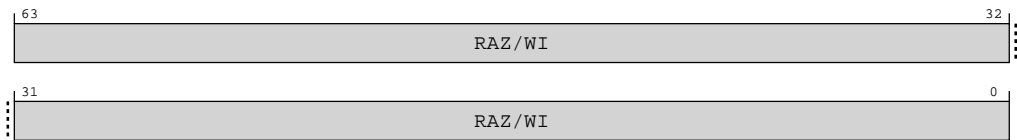


Table A-1243: IMP\_PMCBER\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCBER\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b010

MSR IMP\_PMCBER\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b010

## Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCBER\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCBER_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCBER_EL1;

```

MSR IMP\_PMCBER\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCBER_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCBER_EL1 = X[t, 64];

```

### A.2.11.12 IMP\_PMCPCR\_EL1, STL Program Counter Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

## Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCPCR\_EL1 are UNDEFINED.

## Attributes

### Width

64

### Functional group

Other system control registers

### Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-481: AARCH64\_IMP\_PMCPCCR\_EL1 bit assignments

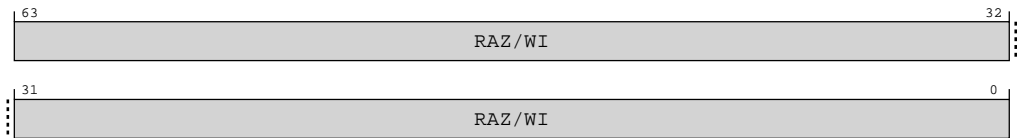


Table A-1246: IMP\_PMCPCCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCPCCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b011

MSR IMP\_PMCPCCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b011

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS &lt;Xt&gt;, IMP\_PMCPCR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCPCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCPCR_EL1;

```

MSR IMP\_PMCPCR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCPCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCPCR_EL1 = X[t, 64];

```

### A.2.11.13 IMP\_PMCHIGHADDR\_EL1, STL High Address Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

#### Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCHIGHADDR\_EL1 are UNDEFINED.

#### Attributes

##### Width

64

##### Functional group

Other system control registers

##### Access type

See bit descriptions

##### Reset value

```

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000

```

Bit descriptions

Figure A-482: AARCH64\_IMP\_PMCHIGHADDR\_EL1 bit assignments

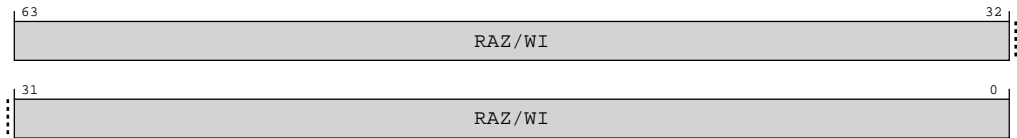


Table A-1249: IMP\_PMCHIGHADDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCHIGHADDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b100

MSR IMP\_PMCHIGHADDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b100

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCHIGHADDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
```

```
    else
        X[t, 64] = IMP_PMCHIGHADDR_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_PMCHIGHADDR_EL1;
```

MSR IMP\_PMCHIGHADDR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCHIGHADDR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_PMCHIGHADDR_EL1 = X[t, 64];
```

A.2.11.14 IMP\_PMCCADDR\_EL1, STL Column Address Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCCADDR\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

Other system control registers

Access type

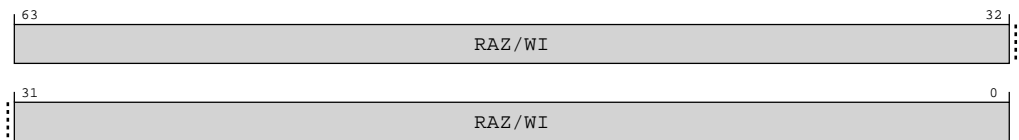
See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-483: AARCH64\_IMP\_PMCCADDR\_EL1 bit assignments



**Table A-1252: IMP\_PMCCADDR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

### Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



#### Note

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCCADDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b101

MSR IMP\_PMCCADDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b101

### Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



#### Note

Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCCADDR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCCADDR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCCADDR_EL1;

```

MSR IMP\_PMCCADDR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);

```



```
else
    IMP_PMCCADDR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCCADDR_EL1 = X[t, 64];
```

A.2.11.15 IMP\_PMCRAADDR\_EL1, STL Row Address register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCRAADDR\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-484: AARCH64\_IMP\_PMCRAADDR\_EL1 bit assignments

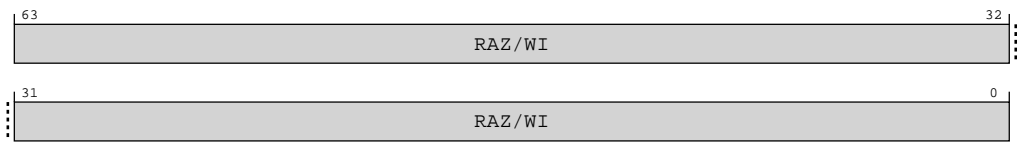


Table A-1255: IMP\_PMCRAADDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCRAADDR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b110

MSR IMP\_PMCRAADDR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b110

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCRAADDR\_EL1

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCRAADDR_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCRAADDR_EL1;
```

MSR IMP\_PMCRAADDR\_EL1, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCRAADDR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_PMCRAADDR_EL1 = X[t, 64];
```

A.2.11.16 IMP\_PMCAR\_EL1, STL Array Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCAR\_EL1 are UNDEFINED.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-485: AARCH64\_IMP\_PMCAR\_EL1 bit assignments

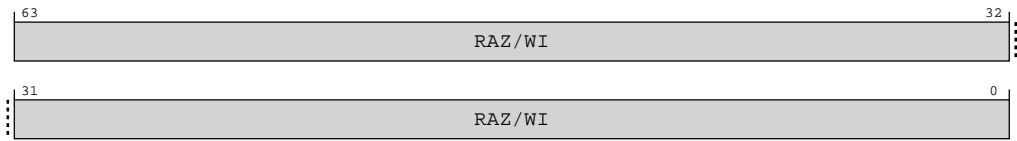


Table A-1258: IMP\_PMCAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCAR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b111

MSR IMP\_PMCAR\_EL1, &lt;Xt&gt;

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1001	0b111

### Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS &lt;Xt&gt;, IMP\_PMCAR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCAR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCAR_EL1;

```

MSR IMP\_PMCAR\_EL1, &lt;Xt&gt;

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCAR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCAR_EL1 = X[t, 64];

```

#### A.2.11.17 IMP\_PMCLCR\_EL1, STL Loop Counter Register

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

### Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCLCR\_EL1 are UNDEFINED.

Attributes

Width  
64

Functional group  
Other system control registers

Access type  
See bit descriptions

Reset value  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure A-486: AARCH64\_IMP\_PMCLCR\_EL1 bit assignments

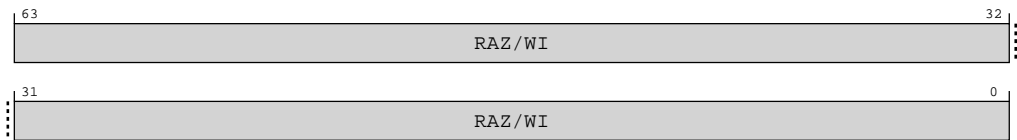



Table A-1261: IMP\_PMCLCR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Note

Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCLCR\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1011	0b111

MSR IMP\_PMCLCR\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1011	0b111

## Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCLCR\_EL1

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCLCR_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCLCR_EL1;

```

MSR IMP\_PMCLCR\_EL1, <Xt>

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCLCR_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCLCR_EL1 = X[t, 64];

```

### A.2.11.18 IMP\_PMCDM<n>\_EL1, STL Data Mask, Fault Bitmap, and Data Registers, n = 0 - 5

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

## Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCDM<n>\_EL1 are UNDEFINED.

## Attributes

### Width

64

### Functional group

Other system control registers

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-487: AARCH64\_IMP\_PMCDM<n>\_EL1 bit assignments

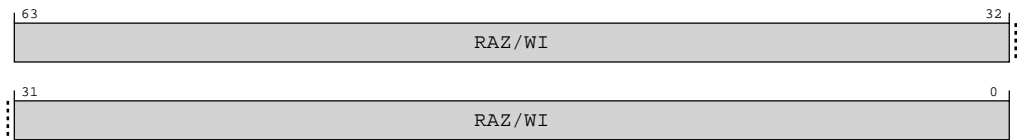


Table A-1264: IMP\_PMCDM<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCDM<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1011	m[2:0]

MSR IMP\_PMCDM<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1011	m[2:0]

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS &lt;Xt&gt;, IMP\_PMCMDM&lt;m&gt;\_EL1

```
integer m = UInt(op2<2:0>);
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCMDM<m>_EL1;
elsif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCMDM<m>_EL1;
```

MSR IMP\_PMCMDM&lt;m&gt;\_EL1, &lt;Xt&gt;

```
integer m = UInt(op2<2:0>);
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCMDM<n>_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    IMP_PMCMDM<n>_EL1 = X[t, 64];
```

#### A.2.11.19 IMP\_PMCXM<n>\_EL1, STL XOR Mask Registers, n = 0 - 5

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

### Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCXM<n>\_EL1 are UNDEFINED.

### Attributes

#### Width

64

#### Functional group

Other system control registers

#### Access type

See bit descriptions

#### Reset value

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```



Bit descriptions

Figure A-488: AARCH64\_IMP\_PMCXM<n>\_EL1 bit assignments

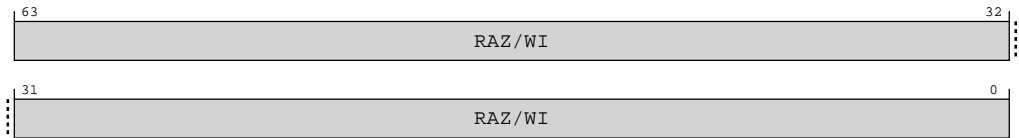


Table A-1267: IMP\_PMCXM<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCXM<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1100	m[2:0]

MSR IMP\_PMCXM<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1100	m[2:0]

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCXM<m>\_EL1

```
integer m = UInt(op2<2:0>);  
  
if PSTATE.EL == EL0 then  
    UNDEFINED;  
elseif PSTATE.EL == EL1 then
```

```

    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCXM<m>_EL1;
    elsif PSTATE.EL == EL2 then
        X[t, 64] = IMP_PMCXM<m>_EL1;

```

MSR IMP\_PMCXM<m>\_EL1, <Xt>

```

integer m = UInt(op2<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCXM<n>_EL1 = X[t, 64];
    elsif PSTATE.EL == EL2 then
        IMP_PMCXM<n>_EL1 = X[t, 64];

```

#### A.2.11.20 IMP\_PMCXM<n>\_EL1, STL Program Registers, n = 0 - 13

Reserved for the STL use. This register has no effect when AArch64-IMP\_TESTR1\_EL1.E is set to 0b0.

#### Configurations

This register is present only when PMC == 1. Otherwise, direct accesses to IMP\_PMCXM<n>\_EL1 are UNDEFINED.

#### Attributes

##### Width

64

##### Functional group

Other system control registers

##### Access type

See bit descriptions

##### Reset value

0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000

Bit descriptions

Figure A-489: AARCH64\_IMP\_PMCP<n>\_EL1 bit assignments

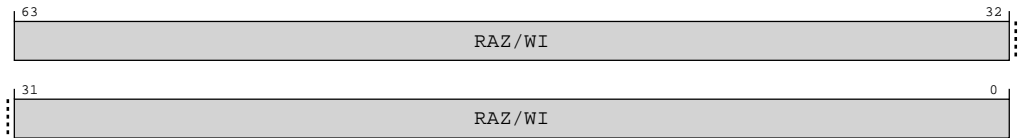


Table A-1270: IMP\_PMCP<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RAZ/WI	Reserved	RAZ/WI

Access

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is **RAZ/WI**.



Writing to this register might cause **UNPREDICTABLE** behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCP<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1101	m[2:0]

MRS <Xt>, IMP\_PMCP<m>\_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1110	m[2:0]

MSR IMP\_PMCP<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1101	m[2:0]

MSR IMP\_PMCP<m>\_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b1111	0b1110	m[2:0]

Accessibility

When AArch64-IMP\_TESTR1\_EL1.E is set to 0b0, the access to this register is RAZ/WI.



Writing to this register might cause UNPREDICTABLE behaviors. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

MRS <Xt>, IMP\_PMCP<m>\_EL1

```
integer m = UInt(op2<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCP<m>_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCP<m>_EL1;
```

MRS <Xt>, IMP\_PMCP<m>\_EL1

```
integer m = UInt(op2<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        X[t, 64] = IMP_PMCP<m>_EL1;
elseif PSTATE.EL == EL2 then
    X[t, 64] = IMP_PMCP<m>_EL1;
```

MSR IMP\_PMCP<m>\_EL1, <Xt>

```
integer m = UInt(op2<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCP<n>_EL1 = X[t, 64];
elseif PSTATE.EL == EL2 then
    IMP_PMCP<n>_EL1 = X[t, 64];
```

MSR IMP\_PMCP<m>\_EL1, <Xt>

```
integer m = UInt(op2<2:0>);

if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    if HCR_EL2.TIDCP == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        IMP_PMCP<n>_EL1 = X[t, 64];
```

```
elseif PSTATE.EL == EL2 then
    IMP_P MCP<n>_EL1 = X[t, 64];
```

A.2.11.21 SCTRL\_EL2, System Control Register (EL2)

Provides top level control of the system, including its memory system, at EL2.

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Other system control registers

Access type

See bit descriptions

Reset value

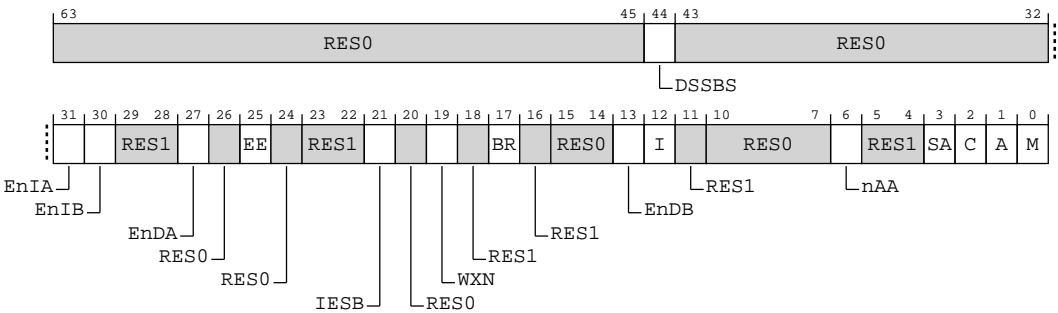
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx0x	xxx0	xxxx	xxxx	x0x0
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-490: AARCH64\_SCTRL\_EL2 bit assignments



**Table A-1275: SCTLR\_EL2 bit descriptions**

Bits	Name	Description	Reset
[63:45]	<b>RES0</b>	Reserved	<b>RES0</b>
[44]	<b>DSSBS</b>	Default PSTATE.SSBS value on Exception Entry.  <b>0b0</b> PSTATE.SSBS is set to 0 on an exception to EL2.  <b>0b1</b> PSTATE.SSBS is set to 1 on an exception to EL2.	<b>x</b>
[43:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31]	<b>EnIA</b>	Controls enabling of pointer authentication of instruction addresses, using the APIAKey_EL1 key, in the EL2 or EL2&0 translation regime.  <b>0b0</b> Pointer authentication of instruction addresses, using the APIAKey_EL1 key, is not enabled.  <b>0b1</b> Pointer authentication of instruction addresses, using the APIAKey_EL1 key, is enabled.  <b>Note:</b> This field controls the behavior of the AddPACIA and AuthIA pseudocode functions. Specifically, when the field is 1, AddPACIA returns a copy of a pointer to which a pointer authentication code has been added, and AuthIA returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b> .	<b>x</b>
[30]	<b>EnIB</b>	Controls enabling of pointer authentication of instruction addresses, using the APIBKey_EL1 key, in the EL2 or EL2&0 translation regime.  <b>0b0</b> Pointer authentication of instruction addresses, using the APIBKey_EL1 key, is not enabled.  <b>0b1</b> Pointer authentication of instruction addresses, using the APIBKey_EL1 key, is enabled.  <b>Note:</b> This field controls the behavior of the AddPACIB and AuthIB pseudocode functions. Specifically, when the field is 1, AddPACIB returns a copy of a pointer to which a pointer authentication code has been added, and AuthIB returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b> .	<b>x</b>
[29:28]	<b>RES1</b>	Reserved	<b>RES1</b>
[27]	<b>EnDA</b>	Controls enabling of pointer authentication of instruction addresses, using the APDAKey_EL1 key, in the EL2 or EL2&0 translation regime.  <b>0b0</b> Pointer authentication of data addresses, using the APDAKey_EL1 key, is not enabled.  <b>0b1</b> Pointer authentication of data addresses, using the APDAKey_EL1 key, is enabled.  <b>Note:</b> This field controls the behavior of the AddPACDA and AuthDA pseudocode functions. Specifically, when the field is 1, AddPACDA returns a copy of a pointer to which a pointer authentication code has been added, and AuthDA returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b> .	<b>x</b>
[26]	<b>RES0</b>	Reserved	<b>RES0</b>

Bits	Name	Description	Reset
[25]	EE	Endianness of data accesses at EL2.  <b>0b0</b> Explicit data accesses at EL2 are little-endian.  <b>0b1</b> Explicit data accesses at EL2 are big-endian.  The EE bit is permitted to be cached in a TLB.	x
[24]	RES0	Reserved	RES0
[23:22]	RES1	Reserved	RES1
[21]	IESB	Implicit Error Synchronization event enable.  <b>0b0</b> Disabled.  <b>0b1</b> An implicit error synchronization event is added: <ul style="list-style-type: none"> <li>At each exception taken to EL2.</li> <li>Before the operational pseudocode of each <b>ERET</b> instruction executed at EL2.</li> </ul> When the PE is in Debug state, this field has no effect.	x
[20]	RES0	Reserved	RES0
[19]	WXN	Write permission implies XN (Execute-never). For the EL2 or EL2&O translation regime, this bit can force all memory regions that are writable to be treated as XN.  <b>0b0</b> This control has no effect on memory access permissions.  <b>0b1</b> Any region that is writable in the EL2 or EL2&O translation regime is forced to XN for accesses from software executing at EL2.  This bit applies only when SCTL_R_EL2.M bit is set.  The WXN bit is permitted to be cached in a TLB.	x
[18]	RES1	Reserved	RES1
[17]	BR	Background region enable for EL2 MPU memory regions.  <b>0b0</b> Background region disabled for stage 1 EL2 translation regime and stage 2 EL1&O translation regime.  <b>0b1</b> Background region enabled for stage 1 EL2 translation regime and stage 2 EL1&O translation regime.  If EL2 MPU is enabled, then EL0 and EL1 access that does not match an EL2 MPU region always results in a Translation fault.	0b0
[16]	RES1	Reserved	RES1
[15:14]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[13]	EnDB	Controls enabling of pointer authentication of instruction addresses, using the APDBKey_EL1 key, in the EL2 or EL2&0 translation regime.  <b>0b0</b> Pointer authentication of data addresses, using the APDBKey_EL1 key, is not enabled.  <b>0b1</b> Pointer authentication of data addresses, using the APDBKey_EL1 key, is enabled.  <b>Note:</b> This field controls the behavior of the AddPACDB and AuthDB pseudocode functions. Specifically, when the field is 1, AddPACDB returns a copy of a pointer to which a pointer authentication code has been added, and AuthDB returns an authenticated copy of a pointer. When the field is 0, both of these functions are <b>NOP</b> .	x
[12]	I	Instruction access Cacheability control, for accesses at EL2.  <b>0b0</b> All instruction accesses to Normal memory from EL2 are Non-cacheable for all levels of instruction and unified cache.  If SCTLR_EL2.{BR, M} == {0, 0}, then instruction accesses from stage 1 of the EL2 translation regime are to Normal, Outer Shareable, Inner Non-cacheable, Outer Non-cacheable memory.  <b>0b1</b> This control has no effect on the Cacheability of instruction access to Normal memory from EL2.  If SCTLR_EL2.{BR, M} = {0, 0}, then instruction accesses from stage 1 of the EL2 translation regime are to Normal, Outer Shareable, Inner Write-Through, Outer Write-Through memory.  This bit has no effect on the EL1&0 translation regime.	0b0
[11]	RES1	Reserved	RES1
[10:7]	RES0	Reserved	RES0
[6]	nAA	Non-aligned access. This bit controls generation of Alignment faults at EL2 under certain conditions.  The following instructions generate an Alignment fault if all bytes being accessed are not within a single 16-byte quantity, aligned to 16 bytes for access: <ul style="list-style-type: none"> <li>• LDAPR, LDAPRH, LDAPUR, LDAPURH, LDAPURSH, LDAPURSW, LDAR, LDARH, LDLAR, LDLARH.</li> <li>• STLLR, STLLRH, STLR, STLRH, STLUR, and STLURH</li> </ul> <b>0b0</b> Unaligned accesses by the specified instructions generate an Alignment fault.  <b>0b1</b> Unaligned accesses by the specified instructions do not generate an Alignment fault.	x
[5:4]	RES1	Reserved	RES1
[3]	SA	SP Alignment check enable. When set to 1, if a load or store instruction executed at EL2 uses the SP as the base address and the SP is not aligned to a 16-byte boundary, then an SP alignment fault exception is generated. For more information, see <i>SP alignment checking</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x



Bits	Name	Description	Reset
[2]	C	<p>Data access Cacheability control, for accesses at EL2.</p> <p><b>0b0</b></p> <p>All data accesses to Normal memory from EL2 are Non-cacheable for all levels of data and unified cache.</p> <p><b>0b1</b></p> <p>This control has no effect on the Cacheability of data accesses to Normal memory from EL2.</p> <p>This bit has no effect on the EL1&amp;0 translation regime.</p>	0b0
[1]	A	<p>Alignment check enable. This is the enable bit for Alignment fault checking at EL2.</p> <p><b>0b0</b></p> <p>Alignment fault checking is disabled when executing at EL2.</p> <p>Alignment checks on some instructions are not disabled by this control. For more information, see <i>Alignment of data accesses</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b1</b></p> <p>Alignment fault checking is enabled when executing at EL2.</p> <p>All instructions that load or store one or more registers have an alignment check that the address being accessed is aligned to the size of the data element(s) being accessed. If this check fails it causes an Alignment fault, which is taken as a Data Abort exception.</p>	x
[0]	M	<p>MPU enable for EL2 stage 1 and EL1&amp;0 stage 2 address translation.</p> <p><b>0b0</b></p> <p>MPU disabled for EL2 and EL1&amp;0 stage 2 address translation.</p> <p>See the SCTLR_EL2.I field for the behavior of instruction accesses to Normal memory.</p> <p><b>0b1</b></p> <p>MPU enabled for EL2 and EL1&amp;0 stage 2 address translation.</p>	0b0

## Access

MRS <Xt>, SCTLR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0000	0b000

MSR SCTLR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0000	0b000

## Accessibility

MRS <Xt>, SCTLR\_EL2

```

if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = SCTLR_EL2;

```

MSR SCTLR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    SCTLR_EL2 = X[t, 64];
```

A.2.11.22 HSTR\_EL2, Hypervisor System Trap Register

Controls trapping to EL2 of EL1 or lower AArch32 accesses to the System register in the coproc == 0b1111 encoding space, by the CRn value used to access the register using MCR or MRC instruction. When the register is accessible using an MCRR or MRRC instruction, this is the CRm value used to access the register.

Configurations

This register is available in all configurations.

Attributes

Width

64

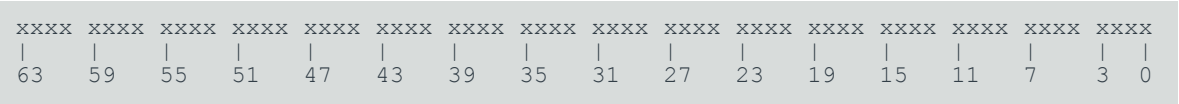
Functional group

Other system control registers

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure A-491: AARCH64\_HSTR\_EL2 bit assignments

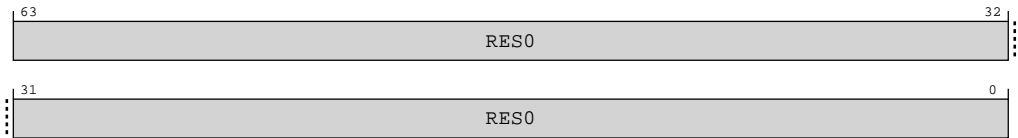


Table A-1278: HSTR\_EL2 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

MRS <Xt>, HSTR\_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b011

MSR HSTR\_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0001	0b0001	0b011

Accessibility

MRS <Xt>, HSTR\_EL2

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    X[t, 64] = HSTR_EL2;
```

MSR HSTR\_EL2, <Xt>

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elseif PSTATE.EL == EL1 then
    UNDEFINED;
elseif PSTATE.EL == EL2 then
    HSTR_EL2 = X[t, 64];
```

## Appendix B External registers

This appendix contains the descriptions for all the external (memory-mapped) registers in the Cortex®-R82AE processor.

### B.1 Registers accessed over the Utility bus

This section contains the summary and descriptions for all the external registers in the Cortex®-R82AE processor accessed over the Utility bus.

Utility bus implements one of two memory maps:

- A sparse memory map, when the configuration parameter `DENSE_CS_ADDR_MAP` is 0. Each set of System registers is grouped on separate 64KB page boundaries. This allows to isolate and remap components when using the EL1 MMU (if VMSA included) with the maximum 64KB granule.
- A dense memory map, when the configuration parameter `DENSE_CS_ADDR_MAP` is 1. Each set of System registers is grouped on separate 4KB page boundaries. It may not be possible to isolate and remap individual components using an EL1 MMU with 16KB or 64KB granules. You can either use a 4KB granule, or depend on an EL2 MPU (or an EL1 MPU, if EL1 is using PMSA) to isolate components without remapping.

The following table shows the total space occupied by the Utility bus memory map, depending on how many cores are implemented in the processor.

**Table B-1: Utility bus sparse and dense memory map sizes**

Number of cores	Sparse memory map	Dense memory map
1	20-bit (1MB)	15-bit (32KB)
2	21-bit (2MB)	15-bit (32KB)
3	22-bit (4MB)	16-bit (64KB)
4	22-bit (4MB)	16-bit (64KB)
5	23-bit (8MB)	17-bit (128KB)
6	23-bit (8MB)	17-bit (128KB)
7	23-bit (8MB)	17-bit (128KB)
8	23-bit (8MB)	17-bit (128KB)

The following table shows the base addresses for each set of system component registers that the external agents can access using the Utility bus.



Note

- In the following table, any address space that is not documented or that corresponds to non-implemented cores is treated as **RAZ/WI**.
- The base addresses in the following table are the addresses accessed on the Utility bus interface. The system interconnect typically maps these addresses into a particular address range based on the system address map. Therefore,

software has to add the base address listed here onto the system address range base to get the absolute physical address of a register.

**Table B-2: Memory map for external agents accessing the Utility bus**

Base address, sparse map (DENSE_CS_ADDR_MAP = 0)	Base address, dense map (DENSE_CS_ADDR_MAP = 1)	Registers	Memory map
0x010000	0x01000	Cluster PPU	<a href="#">B.1.1.3 External CLUSTERPPU registers summary</a> on page 1501
0x020000	0x02000	Core 0 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x030000	0x03000	Core 0 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x040000	0x04000	Core 0 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x120000	0x05000	Core 1 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x130000	0x06000	Core 1 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x140000	0x07000	Core 1 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x220000	0x08000	Core 2 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x230000	0x09000	Core 2 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x240000	0x0A000	Core 2 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x320000	0x0B000	Core 3 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x330000	0x0C000	Core 3 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x340000	0x0D000	Core 3 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x420000	0x0E000	Core 4 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x430000	0x0F000	Core 4 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x440000	0x10000	Core 4 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x520000	0x11000	Core 5 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x530000	0x12000	Core 5 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x540000	0x13000	Core 5 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x620000	0x14000	Core 6 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x630000	0x15000	Core 6 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502

Base address, sparse map (DENSE_CS_ADDR_MAP = 0)	Base address, dense map (DENSE_CS_ADDR_MAP = 1)	Registers	Memory map
0x640000	0x16000	Core 6 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x720000	0x17000	Core 7 RAS	<a href="#">B.1.1.1 External RAS registers summary</a> on page 1498
0x730000	0x18000	Core 7 SBIST Controller	<a href="#">B.1.1.5 External SBISTC registers summary</a> on page 1502
0x740000	0x19000	Core 7 PPU	<a href="#">B.1.1.2 External PPU registers summary</a> on page 1499
0x050000	0x1A000	Cluster MBIST Controller 0	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x060000	0x1B000	Cluster MBIST Controller 1	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x070000	0x1C000	Core 0 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x170000	0x1D000	Core 1 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x170000	0x1D000	Core 1 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x270000	0x1E000	Core 2 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x370000	0x1F000	Core 3 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x470000	0x20000	Core 4 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x570000	0x21000	Core 5 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x670000	0x22000	Core 6 MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x770000	0x23000	Core MBIST Controller	Please refer to the <i>Arm® PMC-100 Technical Reference Manual</i>
0x080000	0x24000	Cluster Safety Registers	<a href="#">B.1.1.4 External CLUSTERSAFETY registers summary</a> on page 1502

## B.1.1 Register summaries for registers accessed over the Utility bus

This section includes the summary tables for all the external registers in the Cortex®-R82AE processor accessed over the Utility bus.

### B.1.1.1 External RAS registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped RAS registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-3: RAS registers summary**

Offset	Name	Reset	Width	Description
0x000 + (64 * n)	<a href="#">ERR&lt;n&gt;FR</a>	See individual bit resets.	64-bit	Error Record <n> Feature Register
0x008 + (64 * n)	<a href="#">ERR&lt;n&gt;CTLR</a>	See individual bit resets.	64-bit	Error Record <n> Control Register
0x010 + (64 * n)	<a href="#">ERR&lt;n&gt;STATUS</a>	See individual bit resets.	64-bit	Error Record <n> Primary Status Register
0x020 + (64 * n)	<a href="#">ERR&lt;n&gt;MISC0</a>	See individual bit resets.	64-bit	Error Record <n> Miscellaneous Register 0
0x028 + (64 * n)	<a href="#">ERR&lt;n&gt;MISC1</a>	See individual bit resets.	64-bit	Error Record <n> Miscellaneous Register 1
0x030 + (64 * n)	<a href="#">ERR&lt;n&gt;MISC2</a>	See individual bit resets.	64-bit	Error Record <n> Miscellaneous Register 2
0x038 + (64 * n)	<a href="#">ERR&lt;n&gt;MISC3</a>	See individual bit resets.	64-bit	Error Record <n> Miscellaneous Register 3
0x800 + (64 * n)	<a href="#">ERR&lt;n&gt;PFGF</a>	See individual bit resets.	64-bit	Error Record <n> Pseudo-fault Generation Feature Register
0x808 + (64 * n)	<a href="#">ERR&lt;n&gt;PFGCTL</a>	See individual bit resets.	64-bit	Error Record <n> Pseudo-fault Generation Control Register
0x810 + (64 * n)	<a href="#">ERR&lt;n&gt;PFGCDN</a>	See individual bit resets.	64-bit	Error Record <n> Pseudo-fault Generation Countdown Register
0xE00	<a href="#">ERRGSR</a>	See individual bit resets.	64-bit	Error Group Status Register
0xE10	<a href="#">ERRIDR</a>	See individual bit resets.	32-bit	Implementation Identification Register
0xFA8	<a href="#">ERRDEVAFF</a>	See individual bit resets.	64-bit	Device Affinity Register
0xFBC	<a href="#">ERRDEVARCH</a>	See individual bit resets.	32-bit	Device Architecture Register
0xFC8	<a href="#">ERRDEVID</a>	See individual bit resets.	32-bit	Device Configuration Register
0xFD0	<a href="#">ERRPIDR4</a>	See individual bit resets.	32-bit	Peripheral Identification Register 4
0xFE0	<a href="#">ERRPIDR0</a>	See individual bit resets.	32-bit	Peripheral Identification Register 0
0xFE4	<a href="#">ERRPIDR1</a>	See individual bit resets.	32-bit	Peripheral Identification Register 1
0xFE8	<a href="#">ERRPIDR2</a>	See individual bit resets.	32-bit	Peripheral Identification Register 2
0xFEC	<a href="#">ERRPIDR3</a>	See individual bit resets.	32-bit	Peripheral Identification Register 3
0xFF0	<a href="#">ERRCIDR0</a>	See individual bit resets.	32-bit	Component Identification Register 0
0xFF4	<a href="#">ERRCIDR1</a>	See individual bit resets.	32-bit	Component Identification Register 1
0xFF8	<a href="#">ERRCIDR2</a>	See individual bit resets.	32-bit	Component Identification Register 2
0xFFC	<a href="#">ERRCIDR3</a>	See individual bit resets.	32-bit	Component Identification Register 3

### B.1.1.2 External PPU registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped PPU registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-4: PPU registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">PPU_PWPR</a>	See individual bit resets.	32-bit	Power Policy Register
0x004	<a href="#">PPU_PMER</a>	See individual bit resets.	32-bit	Power Mode Emulation Enable Register
0x008	<a href="#">PPU_PWSR</a>	See individual bit resets.	32-bit	Power Status Register
0x010	<a href="#">PPU_DISR</a>	See individual bit resets.	32-bit	Device Interface Input Current Status Register
0x014	<a href="#">PPU_MISR</a>	See individual bit resets.	32-bit	Miscellaneous Input Current Status Register
0x018	<a href="#">PPU_STSR</a>	See individual bit resets.	32-bit	Stored Status Register
0x01C	<a href="#">PPU_UNLK</a>	See individual bit resets.	32-bit	Unlock Register
0x020	<a href="#">PPU_PWCR</a>	See individual bit resets.	32-bit	Power Configuration Register
0x024	<a href="#">PPU_PTCR</a>	See individual bit resets.	32-bit	Power Mode Transition Register
0x030	<a href="#">PPU_IMR</a>	See individual bit resets.	32-bit	Interrupt Mask Register
0x034	<a href="#">PPU_AIMR</a>	See individual bit resets.	32-bit	Additional Interrupt Mask Register
0x038	<a href="#">PPU_ISR</a>	See individual bit resets.	32-bit	Interrupt Status Register
0x03C	<a href="#">PPU_AISR</a>	See individual bit resets.	32-bit	Additional Interrupt Status Register
0x040	<a href="#">PPU_IESR</a>	See individual bit resets.	32-bit	Input Edge Sensitivity Register
0x044	<a href="#">PPU_OPSR</a>	See individual bit resets.	32-bit	Operating Mode Active Edge Sensitivity Register
0x050	<a href="#">PPU_FUNRR</a>	See individual bit resets.	32-bit	Functional Retention RAM Configuration Register
0x054	<a href="#">PPU_FULRR</a>	See individual bit resets.	32-bit	Full Retention RAM Configuration Register
0x058	<a href="#">PPU_MEMRR</a>	See individual bit resets.	32-bit	Memory Retention RAM Configuration Register
0x160	<a href="#">PPU_EDTR0</a>	See individual bit resets.	32-bit	Power Mode Entry Delay Register 0
0x164	<a href="#">PPU_EDTR1</a>	See individual bit resets.	32-bit	Power Mode Entry Delay Register 1
0x170	<a href="#">PPU_DCDR0</a>	See individual bit resets.	32-bit	Device Control Delay Configuration Register 0
0x174	<a href="#">PPU_DCDR1</a>	See individual bit resets.	32-bit	Device Control Delay Configuration Register 1
0xFB0	<a href="#">PPU_IDR0</a>	See individual bit resets.	32-bit	PPU Identification Register 0
0xFB4	<a href="#">PPU_IDR1</a>	See individual bit resets.	32-bit	PPU Identification Register 1
0xFC8	<a href="#">PPU_IIDR</a>	See individual bit resets.	32-bit	Implementation Identification Register
0xFCC	<a href="#">PPU_AIDR</a>	See individual bit resets.	32-bit	Architecture Identification Register
0xFD0	<a href="#">PPU_PIDR4</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 4
0xFD4	<a href="#">PPU_PIDR5</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 5
0xFD8	<a href="#">PPU_PIDR6</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 6
0xFDC	<a href="#">PPU_PIDR7</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 7



Offset	Name	Reset	Width	Description
0xFE0	<a href="#">PPU_PIDR0</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 0
0xFE4	<a href="#">PPU_PIDR1</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 1
0xFE8	<a href="#">PPU_PIDR2</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 2
0xFEC	<a href="#">PPU_PIDR3</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 3
0xFF0	<a href="#">PPU_CIDR0</a>	See individual bit resets.	32-bit	PPU Component Identification Register 0
0xFF4	<a href="#">PPU_CIDR1</a>	See individual bit resets.	32-bit	PPU Component Identification Register 1
0xFF8	<a href="#">PPU_CIDR2</a>	See individual bit resets.	32-bit	PPU Component Identification Register 2
0xFFC	<a href="#">PPU_CIDR3</a>	See individual bit resets.	32-bit	PPU Component Identification Register 3

### B.1.1.3 External CLUSTERPPU registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped CLUSTERPPU registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-5: CLUSTERPPU registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">CLUSTERPPU_PWPR</a>	See individual bit resets.	32-bit	Power Policy Register
0x004	<a href="#">CLUSTERPPU_PMER</a>	See individual bit resets.	32-bit	Power Mode Emulation Enable Register
0x008	<a href="#">CLUSTERPPU_PWSR</a>	See individual bit resets.	32-bit	Power Status Register
0x010	<a href="#">CLUSTERPPU_DISR</a>	See individual bit resets.	32-bit	Device Interface Input Current Status Register
0x014	<a href="#">CLUSTERPPU_MISR</a>	See individual bit resets.	32-bit	Miscellaneous Input Current Status Register
0x018	<a href="#">CLUSTERPPU_STSR</a>	See individual bit resets.	32-bit	Stored Status Register
0x01C	<a href="#">CLUSTERPPU_UNLK</a>	See individual bit resets.	32-bit	Unlock Register
0x020	<a href="#">CLUSTERPPU_PWCR</a>	See individual bit resets.	32-bit	Power Configuration Register
0x024	<a href="#">CLUSTERPPU_PTCR</a>	See individual bit resets.	32-bit	Power Mode Transition Register
0x030	<a href="#">CLUSTERPPU_IMR</a>	See individual bit resets.	32-bit	Interrupt Mask Register
0x034	<a href="#">CLUSTERPPU_AIMR</a>	See individual bit resets.	32-bit	Additional Interrupt Mask Register
0x038	<a href="#">CLUSTERPPU_ISR</a>	See individual bit resets.	32-bit	Interrupt Status Register
0x03C	<a href="#">CLUSTERPPU_AISR</a>	See individual bit resets.	32-bit	Additional Interrupt Status Register
0x040	<a href="#">CLUSTERPPU_IESR</a>	See individual bit resets.	32-bit	Input Edge Sensitivity Register
0x044	<a href="#">CLUSTERPPU_OPSR</a>	See individual bit resets.	32-bit	Operating Mode Active Edge Sensitivity Register
0x050	<a href="#">CLUSTERPPU_FUNRR</a>	See individual bit resets.	32-bit	Functional Retention RAM Configuration Register
0x054	<a href="#">CLUSTERPPU_FULRR</a>	See individual bit resets.	32-bit	Full Retention RAM Configuration Register
0x058	<a href="#">CLUSTERPPU_MEMRR</a>	See individual bit resets.	32-bit	Memory Retention RAM Configuration Register
0x160	<a href="#">CLUSTERPPU_EDTRO</a>	See individual bit resets.	32-bit	Power Mode Entry Delay Register 0

Offset	Name	Reset	Width	Description
0x164	<a href="#">CLUSTERPPU_EDTR1</a>	See individual bit resets.	32-bit	Power Mode Entry Delay Register 1
0x170	<a href="#">CLUSTERPPU_DCDR0</a>	See individual bit resets.	32-bit	Device Control Delay Configuration Register 0
0x174	<a href="#">CLUSTERPPU_DCDR1</a>	See individual bit resets.	32-bit	Device Control Delay Configuration Register 1
0xFB0	<a href="#">CLUSTERPPU_IDR0</a>	See individual bit resets.	32-bit	PPU Identification Register 0
0xFB4	<a href="#">CLUSTERPPU_IDR1</a>	See individual bit resets.	32-bit	PPU Identification Register 1
0xFC8	<a href="#">CLUSTERPPU_IIDR</a>	See individual bit resets.	32-bit	Implementation Identification Register
0xFCC	<a href="#">CLUSTERPPU_AIDR</a>	See individual bit resets.	32-bit	Architecture Identification Register
0xFD0	<a href="#">CLUSTERPPU_PIDR4</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 4
0xFD4	<a href="#">CLUSTERPPU_PIDR5</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 5
0xFD8	<a href="#">CLUSTERPPU_PIDR6</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 6
0xFDC	<a href="#">CLUSTERPPU_PIDR7</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 7
0xFE0	<a href="#">CLUSTERPPU_PIDR0</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 0
0xFE4	<a href="#">CLUSTERPPU_PIDR1</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 1
0xFE8	<a href="#">CLUSTERPPU_PIDR2</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 2
0xFEC	<a href="#">CLUSTERPPU_PIDR3</a>	See individual bit resets.	32-bit	PPU Peripheral Identification Register 3
0xFF0	<a href="#">CLUSTERPPU_CIDR0</a>	See individual bit resets.	32-bit	CLUSTERPPU Component Identification Register 0
0xFF4	<a href="#">CLUSTERPPU_CIDR1</a>	See individual bit resets.	32-bit	CLUSTERPPU Component Identification Register 1
0xFF8	<a href="#">CLUSTERPPU_CIDR2</a>	See individual bit resets.	32-bit	CLUSTERPPU Component Identification Register 2
0xFFC	<a href="#">CLUSTERPPU_CIDR3</a>	See individual bit resets.	32-bit	CLUSTERPPU Component Identification Register 3

#### B.1.1.4 External CLUSTERSAFETY registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped CLUSTERSAFETY registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-6: CLUSTERSAFETY registers summary**

Offset	Name	Reset	Width	Description
0x060	<a href="#">CLUSTERSAFETY_WRITEKEY</a>	See individual bit resets.	32-bit	PPU Write Key Register

#### B.1.1.5 External SBISTC registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped SBISTC registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-7: SBISTC registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">SBISTC_FCTLR</a>	See individual bit resets.	32-bit	Fault Control Register
0x004	<a href="#">SBISTC_FPIR</a>	See individual bit resets.	32-bit	Fault Partition Identifier Register
0x008	<a href="#">SBISTC_FFMIR</a>	See individual bit resets.	32-bit	Fault Failure Mode Identification Register
0xFBC	<a href="#">SBISTC_DEVARCH</a>	See individual bit resets.	32-bit	Device Architecture Register
0xFC8	<a href="#">SBISTC_IIDR</a>	See individual bit resets.	32-bit	Implementation Identification Register
0xFD0	<a href="#">SBISTC_PIDR4</a>	See individual bit resets.	32-bit	Peripheral Identification Register 4
0xFE0	<a href="#">SBISTC_PIDR0</a>	See individual bit resets.	32-bit	Peripheral Identification Register 0
0xFE4	<a href="#">SBISTC_PIDR1</a>	See individual bit resets.	32-bit	Peripheral Identification Register 1
0xFE8	<a href="#">SBISTC_PIDR2</a>	See individual bit resets.	32-bit	Peripheral Identification Register 2
0xFEC	<a href="#">SBISTC_PIDR3</a>	See individual bit resets.	32-bit	Peripheral Identification Register 3
0xFF0	<a href="#">SBISTC_CIDR0</a>	See individual bit resets.	32-bit	Component Identification Register 0
0xFF4	<a href="#">SBISTC_CIDR1</a>	See individual bit resets.	32-bit	Component Identification Register 1
0xFF8	<a href="#">SBISTC_CIDR2</a>	See individual bit resets.	32-bit	Component Identification Register 2
0xFFC	<a href="#">SBISTC_CIDR3</a>	See individual bit resets.	32-bit	Component Identification Register 3

## B.1.2 Register descriptions for registers accessed over the Utility bus

This section includes the descriptions for all the external registers in the Cortex®-R82AE processor accessed over the Utility bus.

### B.1.2.1 External RAS register description

This section includes the register descriptions for all memory-mapped *Reliability, Availability, and Serviceability* (RAS) registers that are accessed for each core in the Cortex®-R82AE processor.

#### B.1.2.1.1 ERR<n>FR, Error Record <n> Feature Register, n = 0 - 9

Defines whether error record <n> is the first record owned by a node:

- If error record <n> is the first error record owned by a node, then ERR<n>FR.ED is not 0b00.
- If error record <n> is not the first error record owned by a node, then ERR<n>FR.ED is 0b00.

If error record <n> is the first record owned by the node, defines which of the common architecturally-defined features are implemented by the node and, of the implemented features, which are software programmable.

Configurations

Present only if error record <n> is implemented. Otherwise, this register is RES0.

Attributes

Width

64

Component

RAS

Register offset

0x000 + (64 \* n)

Access type


RO

Reset value

When n == 0, or n == 1, or n == 4, or n == 7 or n == 8

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xx00 10xx xx10 xxxx 1001 1010 xx10

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xx00



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

When n == 0, or n == 1, or n == 4, or n == 7 or n == 8

Figure B-1: EXT\_ERR<n>FR bit assignments

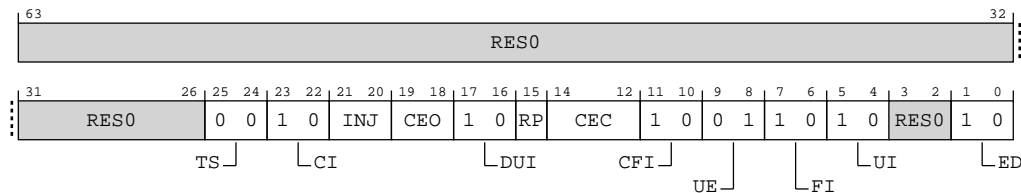


Table B-8: ERR<n>FR bit descriptions

Bits	Name	Description	Reset
[63:26]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[25:24]	TS	<p>Timestamp Extension.</p> <p>Indicates whether, for each error record &lt;m&gt; owned by this node, ERR&lt;m&gt;MISC3 is used as the timestamp register, and, if it is, the timebase used by the timestamp.</p> <p><b>0b00</b></p> <p>The node does not support a timestamp register.</p> <p>All other values are reserved.</p>	0b00
[23:22]	CI	<p>Critical error interrupt.</p> <p>Indicates whether the critical error interrupt and associated controls are implemented.</p> <p><b>0b10</b></p> <p>Critical error interrupt is supported and it can be enabled using associated controls.</p> <p>All other values are reserved.</p>	0b10
[21:20]	INJ	<p><b>When n == 1, or n == 4, or n == 7 or n == 8</b></p> <p>Fault Injection Extension.</p> <p>Indicates whether the RAS Common Fault Injection Model Extension is implemented.</p> <p><b>01</b></p> <p>The node implements the RAS Common Fault Injection Model Extension. See ext-ERR&lt;n&gt;PFGF for more information.</p> <p><b>When n == 0</b></p> <p>Fault Injection Extension.</p> <p>Indicates whether the RAS Common Fault Injection Model Extension is implemented.</p> <p><b>00</b></p> <p>The node does not support the RAS Common Fault Injection Model Extension.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xx
[19:18]	CEO	<p><b>When n == 1 or n == 4</b></p> <p>Corrected Error overwrite. Indicates the behavior of the node when a second or subsequent Corrected error is recorded and a first Corrected error has previously been recorded by an error record &lt;m&gt; owned by the node.</p> <p><b>00</b></p> <p>Keeps the previous error syndrome.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xx
[17:16]	DUI	<p>Error recovery interrupt for deferred errors.</p> <p>Indicates whether the node implements a control for enabling error recovery interrupts on deferred errors.</p> <p><b>0b10</b></p> <p>Feature is controllable using ext-ERR&lt;n&gt;CTLR.DUI.</p>	0b10

Bits	Name	Description	Reset
[15]	RP	<p><b>When n == 1 or n == 4</b></p> <p>Repeat counter. Indicates whether the node implements a second Corrected error counter in ERR&lt;m&gt;MISCO for each error record &lt;m&gt; owned by the node that can record countable errors.</p> <p><b>0</b></p> <p>Implements a single Corrected error counter in ERR&lt;m&gt;MISCO for each error record &lt;m&gt; owned by the node that can record countable errors.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[14:12]	CEC	<p><b>When n == 1 or n == 4</b></p> <p>Corrected Error Counter.</p> <p>Indicates whether the node implements standard Corrected error counter (CE counter) mechanisms in ERR&lt;m&gt;MISCO for each error record &lt;m&gt; owned by the node that can record countable errors.</p> <p><b>010</b></p> <p>Implements an 8-bit Corrected error counter in ERR&lt;m&gt;MISCO[39:32].</p> <p><b>When n == 0, or n == 7 or n == 8</b></p> <p>Corrected Error Counter.</p> <p>Indicates whether the node implements standard Corrected error counter (CE counter) mechanisms in ERR&lt;m&gt;MISCO for each error record &lt;m&gt; owned by the node that can record countable errors.</p> <p><b>000</b></p> <p>Does not implement the standard Corrected error counter model.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xxx
[11:10]	CFI	<p>Fault handling interrupt for corrected errors.</p> <p>Indicates whether the node implements a control for enabling fault handling interrupts on corrected errors.</p> <p><b>0b10</b></p> <p>Feature is controllable using ext-ERR&lt;n&gt;CTLR.CFI.</p>	0b10
[9:8]	UE	<p>In-band uncorrected error reporting.</p> <p>Indicates whether the node implements in-band uncorrected error reporting (External aborts), and, if so, whether the node implements controls for enabling and disabling the reporting.</p> <p><b>0b01</b></p> <p>Feature always enabled. ext-ERR&lt;n&gt;CTLR.UE is <b>RES0</b>.</p>	0b01
[7:6]	FI	<p>Fault handling interrupt.</p> <p>Indicates whether the node implements a fault handling interrupt, and, if so, whether the node implements controls for enabling and disabling the interrupt.</p> <p><b>0b10</b></p> <p>Feature is controllable using ext-ERR&lt;n&gt;CTLR.FI.</p>	0b10
[5:4]	UI	<p>Error recovery interrupt for uncorrected errors.</p> <p>Indicates whether the node implements an error recovery interrupt, and, if so, whether the node implements controls for enabling and disabling the interrupt.</p> <p><b>0b10</b></p> <p>Feature is controllable using ext-ERR&lt;n&gt;CTLR.UI.</p>	0b10

Bits	Name	Description	Reset
[3:2]	RES0	Reserved	RES0
[1:0]	ED	Error reporting and logging.  Indicates whether <n> is the first record owned by the node, and, if it is, whether the node implements controls for enabling and disabling error reporting and logging.  <b>0b10</b>  Feature is controllable using ext-ERR<n>CTLR.ED.	0b10

Figure B-2: EXT\_ERR<n>FR bit assignments

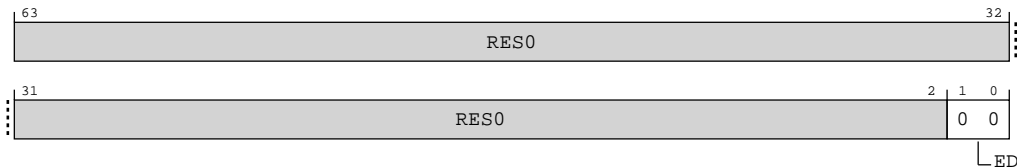


Table B-9: ERR<n>FR bit descriptions

Bits	Name	Description	Reset
[63:2]	RES0	Reserved	RES0
[1:0]	ED	Error reporting and logging.  Indicates whether <n> is the first record owned by the node, and, if it is, whether the node implements controls for enabling and disabling error reporting and logging.  <b>0b00</b>  Error record <n> is not the first record owned by the node.	0b00

Accessibility

Component	Offset	Instance	Range
RAS	0x000 + (64 * n)	ERR<n>FR	None

This interface is accessible as follows:

RO

B.1.2.1.2 ERR<n>CTLR, Error Record <n> Control Register, n = 0 - 9

The error control register contains enable bits for the node that writes to this record:

- Enabling error detection and correction.
- Enabling the critical error, error recovery, and fault handling interrupts.
- Enabling in-band error response for uncorrected errors.

For each bit, if the node does not support the feature, then the bit is **RES0**. The definition of each record is IMPLEMENTATION DEFINED.

Configurations

If error record <n> is not implemented, or error record <n> is not the first error record owned by the node, ERR<n>CTLR is RES0.

ext-ERR<n>FR describes the features implemented by the node.

Attributes

Width

64

Component

RAS

Register offset

0x008 + (64 \* n)

Access type

RW

Reset value

When n == 0, or n == 1, or n == 4, or n == 7 or n == 8

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xx0x x0x0 xxxx 00x0  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When n == 0, or n == 1, or n == 4, or n == 7 or n == 8

Figure B-3: EXT\_ERR<n>CTLR bit assignments

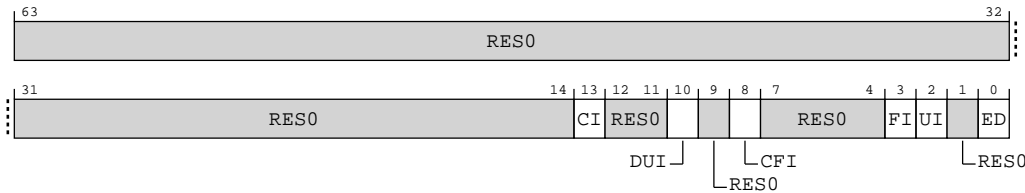


Table B-11: ERR<n>CTLR bit descriptions

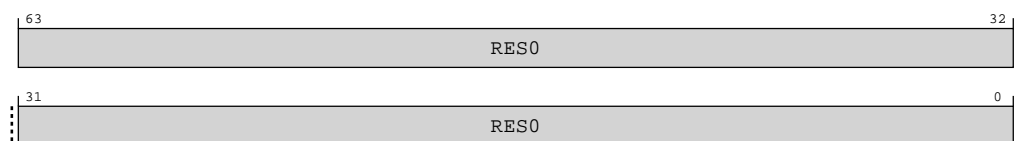
Bits	Name	Description	Reset
[63:14]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[13]	CI	<p>Critical error interrupt enable.</p> <p>When enabled, the critical error interrupt is generated for a critical error condition.</p> <p><b>0b0</b></p> <p>Critical error interrupt not generated for critical errors. Critical errors are treated as Uncontained errors.</p> <p><b>0b1</b></p> <p>Critical error interrupt generated for critical errors.</p>	0b0
[12:11]	RES0	Reserved	RES0
[10]	DUI	<p>Error recovery interrupt for deferred errors enable. This control applies to errors arising from both reads and writes.</p> <p>When enabled, an error recovery interrupt is generated for all detected Deferred errors.</p> <p><b>0b0</b></p> <p>Error recovery interrupt not generated for deferred errors.</p> <p><b>0b1</b></p> <p>Error recovery interrupt generated for deferred errors.</p> <p>The interrupt is generated even if the error syndrome is discarded because the error record already records a higher priority error.</p>	0b0
[9]	RES0	Reserved	RES0
[8]	CFI	<p>Fault handling interrupt for Corrected errors enable. This control applies to errors arising from both reads and writes.</p> <p>When enabled:</p> <ul style="list-style-type: none"> <li>If the node implements Corrected error counters, then the fault handling interrupt is generated when a counter overflows and the overflow bit for the counter is set to 1. For more information, see ext-ERR&lt;n&gt;MISC0.</li> <li>Otherwise, the fault handling interrupt is generated for all detected Corrected errors.</li> </ul> <p><b>0b0</b></p> <p>Fault handling interrupt not generated for Corrected errors.</p> <p><b>0b1</b></p> <p>Fault handling interrupt generated for Corrected errors.</p> <p>The interrupt is generated even if the error syndrome is discarded because the error record already records a higher priority error.</p>	0b0
[7:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3]	FI	<p>Fault handling interrupt enable. This control applies to errors arising from both reads and writes.</p> <p>When enabled:</p> <ul style="list-style-type: none"> <li>The fault handling interrupt is generated for all detected Deferred errors and Uncorrected errors.</li> <li>If the fault handling interrupt for Corrected errors control is not implemented: <ul style="list-style-type: none"> <li>If the node implements Corrected error counters, then the fault handling interrupt is also generated when a counter overflows and the overflow bit for the counter is set to 1.</li> <li>Otherwise, the fault handling interrupt is also generated for all detected Corrected errors.</li> </ul> </li> </ul> <p><b>0b0</b> Fault handling interrupt disabled.</p> <p><b>0b1</b> Fault handling interrupt enabled.</p> <p>The interrupt is generated even if the error syndrome is discarded because the error record already records a higher priority error.</p>	0b0
[2]	UI	<p>Uncorrected error recovery interrupt enable. This control applies to errors arising from both reads and writes.</p> <p>When enabled, the error recovery interrupt is generated for all detected Uncorrected errors that are not deferred.</p> <p><b>0b0</b> Error recovery interrupt disabled.</p> <p><b>0b1</b> Error recovery interrupt enabled.</p> <p>The interrupt is generated even if the error syndrome is discarded because the error record already records a higher priority error.</p>	0b0
[1]	RES0	Reserved	RES0
[0]	ED	<p>Error reporting and logging enable.</p> <p>When disabled, the node behaves as if error detection and correction are disabled, and no errors are recorded or signaled by the node. Correct error detection and correction codes are written for writes, unless error injection is taking place.</p> <p><b>0b0</b> Error reporting disabled.</p> <p><b>0b1</b> Error reporting enabled.</p> <p>Even when reporting and logging are disabled, the processor still takes all appropriate actions to correct, defer or abort on detected errors.</p>	0b0

Figure B-4: EXT\_ERR&lt;n&gt;CTLR bit assignments



**Table B-12: ERR<n>CTLR bit descriptions**

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

### Accessibility

Component	Offset	Instance	Range
RAS	0x008 + (64 * n)	ERR<n>CTLR	None

This interface is accessible as follows:

RW

#### B.1.2.1.3 ERR<n>STATUS, Error Record <n> Primary Status Register, n = 0 - 9

Contains status information for error record <n>, including:

- Whether any error has been detected (valid).
- Whether any detected error was not corrected, and returned to a Requester.
- Whether any detected error was not corrected and deferred.
- Whether an error record has been discarded because additional errors have been detected before the first error was handled by software (overflow).
- Whether any error has been reported.
- Whether the other error record registers contain valid information.
- Whether the error was reported because poison data was detected or because a corrupt value was detected by an error detection code.
- A primary error code.
- An **IMPLEMENTATION DEFINED** extended error code.

Within this register:

- ERR<n>STATUS.{AV, V, MV} are valid bits that define whether error record <n> registers are valid.
- ERR<n>STATUS.{UE, OF, CE, DE, UET} encode the types of error or errors recorded.
- ERR<n>STATUS.{CI, ER, PN, IERR, SERR} are syndrome fields.

### Configurations

If error record <n> is not implemented, ERR<n>STATUS is RES0.

ERR<q>FR describes the features implemented by the node that owns error record <n>. <q> is the index of the first error record owned by the same node as error record <n>. If the node owns a single record, then q = n.

This register is present only when  $n == 0$ , or  $(n \geq 1 \text{ and } n \leq 6)$  or  $(n \geq 7 \text{ and } n \leq 9)$ . Otherwise, direct accesses to ERR<n>STATUS are UNDEFINED.

Attributes

Width

64

Component

RAS

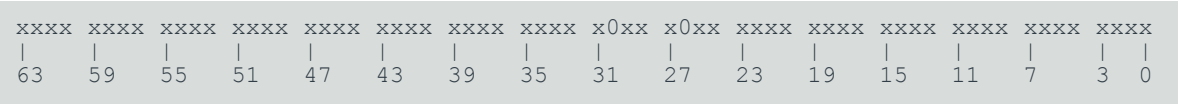
Register offset

0x010 + (64 \* n)

Access type

inconsistent

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-5: EXT\_ERR<n>STATUS bit assignments

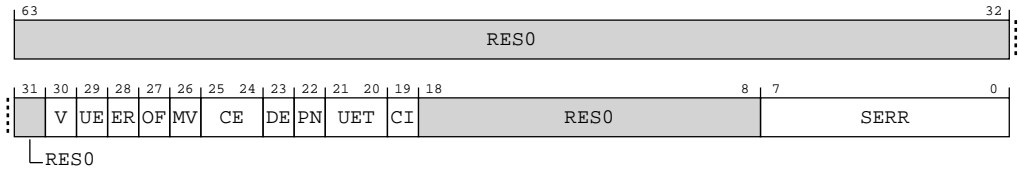


Table B-14: ERR<n>STATUS bit descriptions

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0
[30]	V	Status Register Valid.  0b0 ERR<n>STATUS not valid.  0b1 ERR<n>STATUS valid. At least one error has been recorded.  Access to this field is: W1C	0b0

Bits	Name	Description	Reset
[29]	UE	<p>Uncorrected Error.</p> <p><b>0b0</b></p> <p>No errors have been detected, or all detected errors have been either corrected or deferred.</p> <p><b>0b1</b></p> <p>At least one detected error was not corrected and not deferred.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b></p> <p>Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b></p> <p>Access to this field is: W1C</p>	x
[28]	ER	<p>Error Reported.</p> <p><b>0b0</b></p> <p>No in-band error response (External Abort) signaled to the Requester making the access or other transaction.</p> <p><b>0b1</b></p> <p>An in-band error response was signaled by the component to the Requester making the access or other transaction. This can be because any of the following are true:</p> <ul style="list-style-type: none"> <li>The ERRCTLR[FirstRecordOfNode(n)].UE field, or applicable one of the ERRCTLR[FirstRecordOfNode(n)].{WUE, RUE} fields, is implemented and was 1 when an error was detected and not corrected.</li> <li>The ERRCTLR[FirstRecordOfNode(n)].{WUE, RUE, UE} fields are not implemented and the component always reports errors.</li> </ul> <p>Deferred error will not set this field to 1. When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0' or ext-ERR&lt;n&gt;STATUS.UE == '0'</b></p> <p>Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b></p> <p>Access to this field is: W1C</p>	x

Bits	Name	Description	Reset
[27]	OF	<p>Overflow.</p> <p>Indicates that multiple errors have been detected. This field is set to 1 when one of the following occurs:</p> <ul style="list-style-type: none"> <li>A Corrected error counter is implemented, an error is counted, and the counter overflows.</li> <li>ERR&lt;n&gt;STATUS.V was previously 1, a Corrected error counter is not implemented, and a Corrected error is recorded.</li> <li>ERR&lt;n&gt;STATUS.V was previously 1, and a type of error other than a Corrected error is recorded.</li> </ul> <p>Otherwise, this field is unchanged when an error is recorded.</p> <p>If a Corrected error counter is implemented, then:</p> <ul style="list-style-type: none"> <li>A direct write that modifies the counter overflow flag indirectly might set this field to an <b>UNKNOWN</b> value.</li> <li>A direct write to this field that clears this field to zero might indirectly set the counter overflow flag to an <b>UNKNOWN</b> value.</li> </ul> <p><b>0b0</b></p> <p>Since this field was last cleared to zero, no error syndrome has been discarded and, if a Corrected error counter is implemented, it has not overflowed.</p> <p><b>0b1</b></p> <p>Since this field was last cleared to zero, at least one error syndrome has been discarded or, if a Corrected error counter is implemented, it might have overflowed.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b></p> <p>Access to this field is: <b>UNKNOWN</b>/W1</p> <p><b>Otherwise</b></p> <p>Access to this field is: W1C</p>	x
[26]	MV	<p>Miscellaneous Registers Valid.</p> <p><b>0b0</b></p> <p>ERR&lt;n&gt;MISC&lt;m&gt; not valid.</p> <p><b>0b1</b></p> <p>The contents of the ERR&lt;n&gt;MISC&lt;m&gt; registers contain additional information for an error recorded by this record.</p> <p>Access to this field is: W1C</p>	0b0

Bits	Name	Description	Reset
[25:24]	CE	<p>Corrected Error.</p> <p><b>0b00</b> No errors were corrected.</p> <p><b>0b10</b> At least one error was corrected.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: W1C</p>	xx
[23]	DE	<p>Deferred Error.</p> <p><b>0b0</b> No errors were deferred.</p> <p><b>0b1</b> At least one error was not corrected and deferred.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: W1C</p>	x
[22]	PN	<p>Poison.</p> <p><b>0b0</b> Uncorrected error or Deferred error recorded because a corrupt value was detected, for example, by an error detection code (EDC), or Corrected error recorded.</p> <p><b>0b1</b> Uncorrected error or Deferred error recorded because a poison value was detected.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0' or ext-ERR&lt;n&gt;STATUS.[DE,UE] == '00'</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: W1C</p>	x

Bits	Name	Description	Reset
[21:20]	UET	<p>Uncorrected Error Type. Describes the state of the component after detecting or consuming an Uncorrected error.</p> <p><b>0b00</b> Uncorrected error, Uncontainable error (UC).</p> <p><b>0b01</b> Uncorrected error, Unrecoverable error (UEU).</p> <p><b>0b10</b> Uncorrected error, Latent or Restartable error (UEO).</p> <p><b>0b11</b> Uncorrected error, Signaled or Recoverable error (UER).</p> <p>UER can mean either Signaled or Recoverable error, and UEO can mean either Latent or Restartable error.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write ones to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0' or ext-ERR&lt;n&gt;STATUS.UE == '0'</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: W1C</p>	xx
[19]	CI	<p>Critical Error. Indicates whether a critical error condition has been recorded.</p> <p><b>0b0</b> No critical error condition.</p> <p><b>0b1</b> Critical error condition.</p> <p>When clearing ERR&lt;n&gt;STATUS.V to 0, if this field is nonzero, then Arm recommends that software write 1 to this field to clear this field to zero.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: W1C</p>	x
[18:8]	RES0	Reserved	RES0
[7:0]	SERR	<p>Architecturally-defined primary error code. The primary error code might be used by a fault handling agent to triage an error without requiring device-specific code. For example, to count and threshold corrected errors in software, or generate a short log entry.</p> <p><b>0b00000000</b> No error.</p> <p><b>0b00000010</b> Data value from (non-associative) internal memory. For example, ECC from on-chip SRAM or buffer.</p> <p><b>0b00000110</b> Data value from associative memory. For example, ECC error on cache data.</p> <p><b>0b00000111</b> Address/control value from associative memory. For example, ECC error on cache tag.</p> <p><b>0b00001000</b> Data value from a TLB. For example, ECC error on TLB data.</p>	8 {x}



Bits	Name	Description	Reset
[7:0] continued	SERR	<p><b>0b00001001</b> Address/control value from a TLB. For example, ECC error on TLB tag.</p> <p><b>0b00001010</b> Data value from producer. For example, parity error on write data bus.</p> <p>This value applies when BUS_PROTECTION == 1.</p> <p><b>0b00001011</b> Address/control value from producer. For example, parity error on address bus.</p> <p>This value applies when BUS_PROTECTION == 1.</p> <p><b>0b00010010</b> Error response from Completer of access. For example, error response from cache write-back.</p> <p>This value applies when CHI == 1.</p>	8{x}
[7:0] continued	SERR	<p><b>0b00010011</b> External timeout. For example, timeout on interaction with another component.</p> <p><b>0b00010100</b> Internal timeout. For example, timeout on interface within the component.</p> <p><b>0b00010101</b> Deferred error from Completer not supported at Requester. For example, poisoned data received from the Completer of an access by a Requester that cannot defer the error further.</p> <p><b>0b00011010</b> Other internal error. For example, parity error on internal state of the component that is not covered by another primary error code.</p>	8{x}
[7:0] continued	SERR	<p>All other values are reserved.</p> <p><b>When ext-ERR&lt;n&gt;STATUS.V == '0'</b> Access to this field is: UNKNOWN/WI</p> <p><b>When ext-ERR&lt;n&gt;STATUS.DE == '0', ext-ERR&lt;n&gt;STATUS.UE == '0', ext-ERR&lt;n&gt;STATUS.CE != '00' and ERR&lt;n&gt;STATUS.CE is not being cleared to 0b00 in the same write</b> Access to this field is: RO</p> <p><b>When ext-ERR&lt;n&gt;STATUS.UE == '0', ext-ERR&lt;n&gt;STATUS.DE != '0' and ERR&lt;n&gt;STATUS.DE is not being cleared to 0b0 in the same write</b> Access to this field is: RO</p> <p><b>When ext-ERR&lt;n&gt;STATUS.UE != '0' and ERR&lt;n&gt;STATUS.UE is not being cleared to 0b0 in the same write</b> Access to this field is: RO</p> <p><b>Otherwise</b> Access to this field is: RW</p>	8{x}

## Access

ERR<n>STATUS.{AV, V, UE, ER, OF, MV, CE, DE, PN, UET, CI} are write-one-to-clear (W1C) fields, meaning writes of zero are ignored, and a write of one or all-ones to the field clears the field to zero. ERR<n>STATUS.{IERR, SERR} are read/write (RW) fields, although the set of implemented valid values is **IMPLEMENTATION DEFINED**. See also ext-ERR<n>PFGF.SYN.

After reading ERR<n>STATUS, software must clear the valid fields in the register to allow new errors to be recorded. However, between reading the register and clearing the valid fields, a new error might have overwritten the register. To prevent this error being lost by software, the register prevents updates to fields that might have been updated by a new error.

A write to the register is ignored if all of:

- Any of ERR<n>STATUS.{V, UE, OF, CE, DE} are nonzero before the write.
- The write does not clear the nonzero ERR<n>STATUS.{V, UE, OF, CE, DE} fields to zero by writing ones to the applicable field or fields.

Some of the fields in ERR<n>STATUS are also defined as **UNKNOWN** where certain combinations of ERR<n>STATUS.{V, DE, UE} are zero. The rules for writes to ERR<n>STATUS allow a node to implement such a field as a fixed read-only value.

For example, a write to ERR<n>STATUS when ERR<n>STATUS.V is 1 results in either ERR<n>STATUS.V field being cleared to zero, or ERR<n>STATUS.V not changing. Since all fields in ERR<n>STATUS, other than ERR<n>STATUS.{AV, V, MV}, usually read as **UNKNOWN** values when ERR<n>STATUS.V is zero, this means those fields can be implemented as read-only if applicable.

To ensure correct and portable operation, when software is clearing the valid fields in the register to allow new errors to be recorded, Arm recommends that software:

- Read ERR<n>STATUS and determine which fields need to be cleared to zero.
- Write ones to all the W1C fields that are nonzero in the read value.
- Write zero to all the W1C fields that are zero in the read value.
- Write zero to all the RW fields.

Otherwise, these fields might not have the correct value when a new fault is recorded.

An exception is when the node supports writing to these fields as part of fault injection. See also ext-ERR<n>PFGF.SYN.

## Accessibility

ERR<n>STATUS.{AV, V, UE, ER, OF, MV, CE, DE, PN, UET, CI} are write-one-to-clear (W1C) fields, meaning writes of zero are ignored, and a write of one or all-ones to the field clears the field to zero. ERR<n>STATUS.{IERR, SERR} are read/write (RW) fields, although the set of implemented valid values is IMPLEMENTATION DEFINED. See also ext-ERR<n>PFGF.SYN.

After reading ERR<n>STATUS, software must clear the valid fields in the register to allow new errors to be recorded. However, between reading the register and clearing the valid fields, a new error might have overwritten the register. To prevent this error being lost by software, the register prevents updates to fields that might have been updated by a new error.

A write to the register is ignored if all of:

- Any of ERR<n>STATUS.{V, UE, OF, CE, DE} are nonzero before the write.

- The write does not clear the nonzero ERR<n>STATUS.{V, UE, OF, CE, DE} fields to zero by writing ones to the applicable field or fields.

Some of the fields in ERR<n>STATUS are also defined as UNKNOWN where certain combinations of ERR<n>STATUS.{V, DE, UE} are zero. The rules for writes to ERR<n>STATUS allow a node to implement such a field as a fixed read-only value.

For example, a write to ERR<n>STATUS when ERR<n>STATUS.V is 1 results in either ERR<n>STATUS.V field being cleared to zero, or ERR<n>STATUS.V not changing. Since all fields in ERR<n>STATUS, other than ERR<n>STATUS.{AV, V, MV}, usually read as UNKNOWN values when ERR<n>STATUS.V is zero, this means those fields can be implemented as read-only if applicable.

To ensure correct and portable operation, when software is clearing the valid fields in the register to allow new errors to be recorded, Arm recommends that software:

- Read ERR<n>STATUS and determine which fields need to be cleared to zero.
- Write ones to all the W1C fields that are nonzero in the read value.
- Write zero to all the W1C fields that are zero in the read value.
- Write zero to all the RW fields.

Otherwise, these fields might not have the correct value when a new fault is recorded.

An exception is when the node supports writing to these fields as part of fault injection. See also ext-ERR<n>PFGF.SYN.

Component	Offset	Instance	Range
RAS	0x010 + (64 * n)	ERR<n>STATUS	None

This interface is accessible as follows:

**When ext-ERR<n>STATUS.V != '0' and ERR<n>STATUS.V is not being cleared to 0b0 in the same write**

RO

**When ext-ERR<n>STATUS.UE != '0' and ERR<n>STATUS.UE is not being cleared to 0b0 in the same write**

RO

**When ext-ERR<n>STATUS.OF != '0' and ERR<n>STATUS.OF is not being cleared to 0b0 in the same write**

RO

**When ext-ERR<n>STATUS.CE != '00' and ERR<n>STATUS.CE is not being cleared to 0b00 in the same write**

RO

**When ext-ERR<n>STATUS.DE != '0' and ERR<n>STATUS.DE is not being cleared to 0b0 in the same write**

RO

Otherwise  
RW

B.1.2.1.4 ERR<n>MISC0, Error Record <n> Miscellaneous Register 0, n = 0 - 9

Error syndrome register, containing corrected error counter, FRU identification and other fault state information.

Configurations

If error record <n> is not implemented, ERR<n>MISC0 is RES0.

ERR<q>FR describes the features implemented by the node that owns error record <n>. <q> is the index of the first error record owned by the same node as error record <n>. If the node owns a single record, then q = n.

Attributes

Width

64

Component

RAS

Register offset

0x020 + (64 \* n)

Access type

Read

R

Write

W

Reset value

When n == 0

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When n >= 1 and n <= 3

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When n >= 4 and n <= 6

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

When n == 7, or n == 8 or n == 9

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When  $n == 0$

Figure B-6: EXT\_ERR<n>MISC0 bit assignments

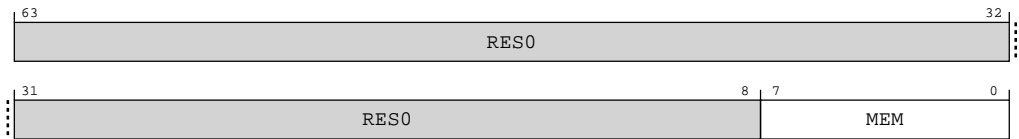
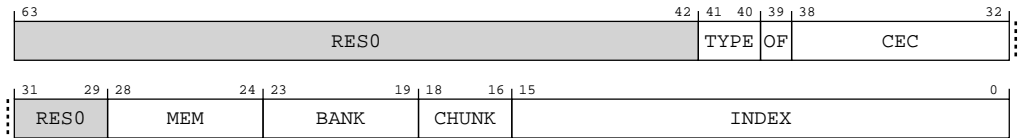


Table B-16: ERR<n>MISC0 bit descriptions

Bits	Name	Description	Reset
[63:8]	RES0	Reserved	RES0
[7:0]	MEM	Indicates which memory encountered the error.  <b>0b01000000</b> Eviction of poisoned cache line to MM, but the port does not support poison.  <b>0b01000011</b> Non-data error response received by MM while attempting an L2 cache line writeback or eviction. The error can be SLVERR or DECERR, if the MM port is configured as AXI, or NDERR if the MM port is configured as CHI. Evictions caused by a Set/Way maintenance operation will return the error to the core and not report the error to RAS.	8 {x}
[7:0] continued	MEM	<b>0b01000100</b> Data error response received by MM with PassDirty attribute set, but the processor is not configured with ECC support, or ECC checking is currently disabled. This occurs when the MM port is configured as CHI and the error is DERR.  This value applies when CHI == 1.  <b>0b00100001</b> Simultaneous MM errors of above types.  Other values are Reserved.	8 {x}

When  $n \geq 1$  and  $n \leq 3$

Figure B-7: EXT\_ERR<n>MISC0 bit assignments

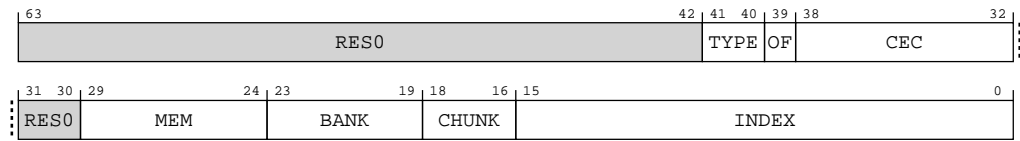


**Table B-17: ERR<n>MISC0 bit descriptions**

Bits	Name	Description	Reset
[63:42]	RES0	Reserved	RES0
[41:40]	TYPE	Error type.  <b>0b00</b> SECEDED scheme detected 1-bit error.  <b>0b01</b> SECEDED scheme detected 2-bit error.  <b>0b10</b> SECEDED scheme detected 1-bit or 2-bit error.	xx
[39]	OF	Sticky overflow bit.  Set to 1 when the Corrected error count field is incremented and wraps through zero.  <b>0b0</b> Counter has not overflowed.  <b>0b1</b> Counter has overflowed.  A direct write that modifies this bit might indirectly set ext-ERR<n>STATUS.OF to an <b>UNKNOWN</b> value and a direct write to ext-ERR<n>STATUS.OF that clears it to zero might indirectly set this bit to an <b>UNKNOWN</b> value.	x
[38:32]	CEC	Corrected error count.  Incremented for each Corrected error. Deferred and Uncorrected errors are not counted.	7 {x}
[31:29]	RES0	Reserved	RES0
[28:24]	MEM	Indicates which memory encountered the error.  <b>0b00001</b> L1 I-cache data error.  <b>0b00010</b> L1 I-cache tag error.  <b>0b00011</b> L1 I-cache simultaneous tag and data errors.	5 {x}
[28:24] continued	MEM	<b>0b01001</b> L1 D-cache data error.  <b>0b01010</b> L1 D-cache tag error.  <b>0b01011</b> L1 D-cache simultaneous tag and data errors.  <b>0b01100</b> L1 D-cache dirty error.  <b>0b01101</b> L1 D-cache simultaneous data and dirty errors.  <b>0b01110</b> L1 D-cache simultaneous tag and dirty errors.	5 {x}

Bits	Name	Description	Reset
[28:24] continued	MEM	<p><b>0b01111</b> L1 D-cache simultaneous tag, data and dirty errors.</p> <p><b>0b10000</b> ITCM error.</p> <p><b>0b10001</b> DTCM error.</p> <p><b>0b11001</b> MMS error data error.</p> <p><b>0b11010</b> MMS error tag error.</p> <p><b>0b11011</b> MMS error simultaneous tag and data errors.</p> <p>Other values are Reserved.</p>	5 {x}
[23:19]	BANK	<p>Indicates which bank within the memory encountered the error.</p> <p>Values in the range 0b00000 - 0b01111 (0x00 - 0x0F) indicate a single bank within the memory specified by the MEM field.</p> <p>Value 0b11111 (0x1F) indicates that simultaneous errors were detected within the memory specified by the MEM field.</p> <p>Other values are Reserved.</p>	5 {x}
[18:16]	CHUNK	<p>Indicates which ECC chunk within the bank encountered the error.</p> <p>Values in the range 0b000 - 0b011 (0x0 - 0x3) indicate a single ECC chunk within the bank specified by the BANK field.</p> <p>Value 0b111 (0x7) indicates that simultaneous errors were detected within the memory specified by the MEM field.</p> <p>Other values are Reserved.</p>	xxx
[15:0]	INDEX	<p>Indicates what was the memory address being accessed when the error occurred.</p> <p>When the MEM field indicates a cache tag, data or dirty memory, the INDEX field indicates the cache line index which was being accessed.</p> <p>When the MEM field indicates ITCM, DTCM, MMS or the L2 buffers, the INDEX field indicates the memory address which was being accessed.</p> <p>Value 0xFFF indicates that simultaneous errors were detected within the memory specified by the MEM field.</p>	16 {x}

When  $n \geq 4$  and  $n \leq 6$

**Figure B-8: EXT\_ERR<n>MISC0 bit assignments****Table B-18: ERR<n>MISC0 bit descriptions**

Bits	Name	Description	Reset
[63:42]	RES0	Reserved	RES0
[41:40]	TYPE	<p>Error type.</p> <p><b>0b00</b> SECEDED scheme detected 1-bit error.</p> <p><b>0b01</b> SECEDED scheme detected 2-bit error.</p> <p><b>0b10</b> SECEDED scheme detected 1-bit or 2-bit error.</p>	xx
[39]	OF	<p>Sticky overflow bit.</p> <p>Set to 1 when the Corrected error count field is incremented and wraps through zero.</p> <p><b>0b0</b> Counter has not overflowed.</p> <p><b>0b1</b> Counter has overflowed.</p> <p>A direct write that modifies this bit might indirectly set ext-ERR&lt;n&gt;STATUS.OF to an <b>UNKNOWN</b> value and a direct write to ext-ERR&lt;n&gt;STATUS.OF that clears it to zero might indirectly set this bit to an <b>UNKNOWN</b> value.</p>	x
[38:32]	CEC	<p>Corrected error count.</p> <p>Incremented for each Corrected error. Deferred and Uncorrected errors are not counted.</p>	7 {x}
[31:30]	RES0	Reserved	RES0
[29:24]	MEM	<p>Indicates which memory encountered the error.</p> <p><b>0b100000</b> L2 cache tag error.</p> <p><b>0b100001</b> L2 cache simultaneous errors in two or more of the following: L2 tags, duplicate L1 tags, data or buffers.</p> <p><b>0b100010</b> L2 cache data error.</p> <p><b>0b100011</b> L2 cache buffers error.</p>	6 {x}



Bits	Name	Description	Reset
[29:24] continued	MEM	<b>0b101000</b> L2 cache core 0 duplicate L1 tag error.  <b>0b101001</b> L2 cache core 1 duplicate L1 tag error.  <b>0b101010</b> L2 cache core 2 duplicate L1 tag error.  <b>0b101011</b> L2 cache core 3 duplicate L1 tag error.  <b>0b101100</b> L2 cache core 4 duplicate L1 tag error.	6{x}
[29:24] continued	MEM	<b>0b101101</b> L2 cache core 5 duplicate L1 tag error.  <b>0b101110</b> L2 cache core 6 duplicate L1 tag error.  <b>0b101111</b> L2 cache core 7 duplicate L1 tag error.  <b>0b110000</b> LCU core 0 duplicate L1 tag error.  <b>0b110001</b> LCU core 1 duplicate L1 tag error.  <b>0b110010</b> LCU core 2 duplicate L1 tag error.  <b>0b110011</b> LCU core 3 duplicate L1 tag error.	6{x}
[29:24] continued	MEM	<b>0b110100</b> LCU core 4 duplicate L1 tag error.  <b>0b110101</b> LCU core 5 duplicate L1 tag error.  <b>0b110110</b> LCU core 6 duplicate L1 tag error.  <b>0b110111</b> LCU core 7 duplicate L1 tag error.  <b>0b111000</b> LCU simultaneous errors in two or more of the duplicate L1 tags.  Other values are Reserved.	6{x}
[23:19]	BANK	Indicates which bank within the memory encountered the error.  Values in the range 0b00000 - 0b01111 (0x00 - 0x0F) indicate a single bank within the memory specified by the MEM field.  Value 0b11111 (0x1F) indicates that simultaneous errors were detected within the memory specified by the MEM field.  Other values are Reserved.	5{x}

Bits	Name	Description	Reset
[18:16]	CHUNK	Indicates which ECC chunk within the bank encountered the error.  Values in the range 0b000 - 0b011 (0x0 - 0x3) indicate a single ECC chunk within the bank specified by the BANK field.  Value 0b111 (0x7) indicates that simultaneous errors were detected within the memory specified by the MEM field.  Other values are Reserved.	xxx
[15:0]	INDEX	Indicates what was the memory address being accessed when the error occurred.  When the MEM field indicates a cache tag, data or dirty memory, the INDEX field indicates the cache line index which was being accessed.  When the MEM field indicates ITCM, DTCM, MMS or the L2 buffers, the INDEX field indicates the memory address which was being accessed.  Value 0xFF indicates that simultaneous errors were detected within the memory specified by the MEM field.	16{x}

When n == 7, or n == 8 or n == 9

Figure B-9: EXT\_ERR<n>MISC0 bit assignments

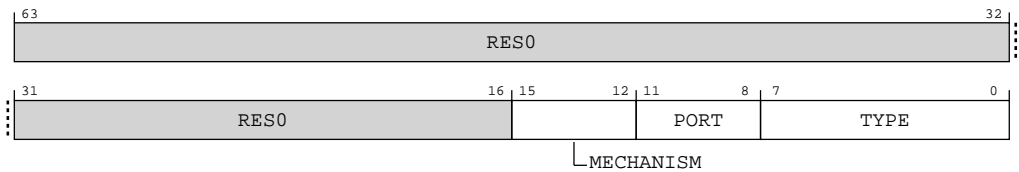


Table B-19: ERR<n>MISC0 bit descriptions

Bits	Name	Description	Reset
[63:16]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[15:12]	MECHANISM	<p>Indicates which bus protection safety mechanism has detected an error.</p> <p><b>0b0000</b> Bus protection.</p> <p><b>0b0001</b> Bus timeout detection.</p> <p><b>0b0010</b> Livelock detection.</p> <p><b>0b0011</b> Masked interrupts timeout detection.</p> <p><b>0b0100</b> WFI/WFE state timeout detection.</p> <p><b>0b0101</b> Transient fault protection.</p> <p>Other values are Reserved.</p>	xxxx
[11:8]	PORT	<p>Indicates which bus port encountered the error.</p> <p><b>0b0000</b> LLPP port error.</p> <p><b>0b0001</b> ACELS port error.</p> <p><b>0b0010</b> LLRAM port error.</p> <p><b>0b0011</b> MM port error.</p> <p><b>0b0100</b> MACP port error.</p> <p><b>0b0101</b> GIC port error.</p> <p><b>0b0110</b> Utility Bus port error.</p> <p><b>0b0111</b> SPP port error.</p> <p><b>0b1000</b> P-Channel port error.</p>	xxxx

Bits	Name	Description	Reset
[11:8] continued	PORT	<p><b>0b1001</b> Q-Channel port error.</p> <p><b>0b1010</b> PPU port error.</p> <p><b>0b1011</b> Configuration port error.</p> <p><b>0b1100</b> Other port error.</p> <p><b>0b1110</b> Not applicable for the error detected by the safety mechanism as indicated by the MECHANISM field.</p> <p><b>0b1111</b> Simultaneous errors detected by multiple ports or multiple mechanisms.</p> <p>Other values are Reserved.</p>	xxxx
[7:0]	TYPE	<p>Indicates the bus error type.</p> <p><b>0b00000000</b> Error on read address channel.</p> <p><b>0b00000001</b> Error on read data channel.</p> <p><b>0b00000010</b> Error on write address channel.</p> <p><b>0b00000011</b> Error on write data channel.</p> <p><b>0b00000100</b> Error on write response channel.</p> <p><b>0b00000101</b> Error on CHI common signals.</p>	8{x}
[7:0] continued	TYPE	<p><b>0b00000110</b> Error on CHI Request channel.</p> <p><b>0b00000111</b> Error on CHI Response channel.</p> <p><b>0b00001000</b> Error on CHI Snoop channel.</p> <p><b>0b00001001</b> Error on CHI Data channel.</p> <p><b>0b00001010</b> Error on Arm GIC interface.</p> <p><b>0b00001011</b> Error on legacy interrupt controller interface.</p> <p><b>0b00001100</b> Error on P-Channel interface.</p>	8{x}

Bits	Name	Description	Reset
[7:0] continued	TYPE	<b>0b00001101</b> Error on Q-Channel interface.  <b>0b00001111</b> Error on miscellaneous interface signals.  <b>0b00010000</b> Core 0 timeout.  <b>0b00010001</b> Core 1 timeout.  <b>0b00010010</b> Core 2 timeout.  <b>0b00010011</b> Core 3 timeout.  <b>0b00010100</b> Core 4 timeout.  <b>0b00010101</b> Core 5 timeout.  <b>0b00010110</b> Core 6 timeout.	8 {x}
[7:0] continued	TYPE	<b>0b00010111</b> Core 7 timeout.  <b>0b00011000</b> LLPP timeout.  <b>0b00011001</b> ACELS timeout.  <b>0b00011010</b> MACP timeout.  <b>0b00011011</b> L2 timeout.  <b>0b00100000</b> Transient fault in DPU.  <b>0b00100001</b> Transient fault in FPU.  <b>0b00100010</b> Transient fault in IFU.	8 {x}

Bits	Name	Description	Reset
[7:0] continued	TYPE	<b>0b00100011</b> Transient fault in L1 data memory system.  <b>0b00100100</b> Transient fault in miscellaneous logic.  <b>0b00111110</b> Not applicable for the error detected by the safety mechanism as indicated by the MECHANISM field.  <b>0b00111111</b> Simultaneous errors detected of different types.  Other values are Reserved.	8 {x}

### Accessibility

When ext-ERR<n>STATUS.MV is set to 1, the miscellaneous syndrome for the most recently recorded error should ignore writes.

Component	Offset	Instance	Range
RAS	0x020 + (64 * n)	ERR<n>MISCO	None

This interface is accessible as follows:

RW

#### B.1.2.1.5 ERR<n>MISC1, Error Record <n> Miscellaneous Register 1, n = 0 - 9

Reserved error syndrome register.

### Configurations

This register is present only when IsErrorRecordImplemented(n). Otherwise, direct accesses to ERR<n>MISC1 are UNDEFINED.

### Attributes

#### Width

64

#### Component

RAS

#### Register offset

0x028 + (64 \* n)

#### Access type

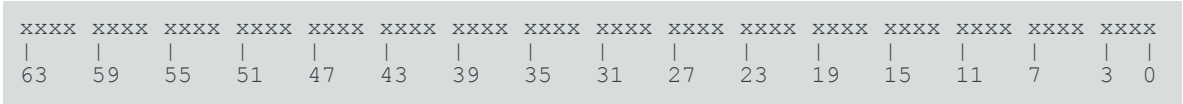
##### Read

R

##### Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-10: EXT\_ERR<n>MISC1 bit assignments

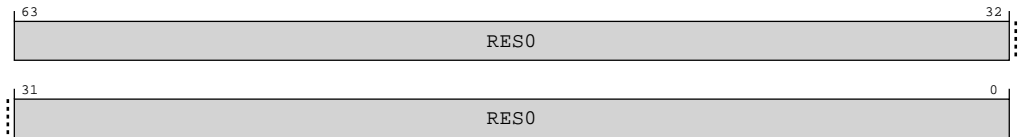


Table B-21: ERR<n>MISC1 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

Reads from ERR<n>MISC1 return an **IMPLEMENTATION DEFINED** value and writes have **IMPLEMENTATION DEFINED** behavior.

If the Common Fault Injection Mechanism is implemented by the node that owns this error record, and ERRPFGF[FirstRecordOfNode(n)].MV is 1, then some parts of this register are read/write when ext-ERR<n>STATUS.MV is 0. See ext-ERR<n>PFGF.MV for more information.

For other parts of this register, or if the Common Fault Injection Mechanism is not implemented, then Arm recommends that:

- Miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.
- When ext-ERR<n>STATUS.MV is 1, the miscellaneous syndrome specific to the most recently recorded error ignores writes.



These recommendations allow a counter to be reset in the presence of a persistent error, while preventing specific information, such as that identifying a FRU, from being lost if an error is detected while the previous error is being logged.

Accessibility

Reads from ERR<n>MISC1 return an IMPLEMENTATION DEFINED value and writes have IMPLEMENTATION DEFINED behavior.

If the Common Fault Injection Mechanism is implemented by the node that owns this error record, and ERRPFGF[FirstRecordOfNode(n)].MV is 1, then some parts of this register are read/write when ext-ERR<n>STATUS.MV is 0. See ext-ERR<n>PFGF.MV for more information.

For other parts of this register, or if the Common Fault Injection Mechanism is not implemented, then Arm recommends that:

- Miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.
- When ext-ERR<n>STATUS.MV is 1, the miscellaneous syndrome specific to the most recently recorded error ignores writes.



These recommendations allow a counter to be reset in the presence of a persistent error, while preventing specific information, such as that identifying a FRU, from being lost if an error is detected while the previous error is being logged.

Component	Offset	Instance	Range
RAS	0x028 + (64 * n)	ERR<n>MISC1	None

This interface is accessible as follows:

RW

B.1.2.1.6 ERR<n>MISC2, Error Record <n> Miscellaneous Register 2, n = 0 - 9

Reserved error syndrome register.

Configurations

This register is present only when IsErrorRecordImplemented(n). Otherwise, direct accesses to ERR<n>MISC2 are UNDEFINED.

Attributes

Width

64

Component

RAS

Register offset

0x030 + (64 \* n)




Access type

Read  
R  
  
Write  
W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

  
Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-11: EXT\_ERR<n>MISC2 bit assignments

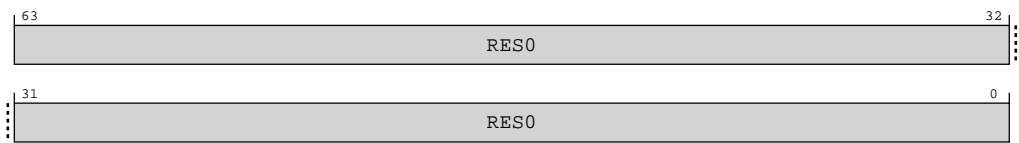


Table B-23: ERR<n>MISC2 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

Reads from ERR<n>MISC2 return an **IMPLEMENTATION DEFINED** value and writes have **IMPLEMENTATION DEFINED** behavior.

If the Common Fault Injection Mechanism is implemented by the node that owns this error record, and ERRPFGF[FirstRecordOfNode(n)].MV is 1, then some parts of this register are read/write when ext-ERR<n>STATUS.MV is 0. See ext-ERR<n>PFGF.MV for more information.

For other parts of this register, or if the Common Fault Injection Mechanism is not implemented, then Arm recommends that:

- Miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.
- When ext-ERR<n>STATUS.MV is 1, the miscellaneous syndrome specific to the most recently recorded error ignores writes.



These recommendations allow a counter to be reset in the presence of a persistent error, while preventing specific information, such as that identifying a FRU, from being lost if an error is detected while the previous error is being logged.

Accessibility

Reads from ERR<n>MISC2 return an IMPLEMENTATION DEFINED value and writes have IMPLEMENTATION DEFINED behavior.

If the Common Fault Injection Mechanism is implemented by the node that owns this error record, and ERRPFGF[FirstRecordOfNode(n)].MV is 1, then some parts of this register are read/write when ext-ERR<n>STATUS.MV is 0. See ext-ERR<n>PFGF.MV for more information.

For other parts of this register, or if the Common Fault Injection Mechanism is not implemented, then Arm recommends that:

- Miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.
- When ext-ERR<n>STATUS.MV is 1, the miscellaneous syndrome specific to the most recently recorded error ignores writes.



These recommendations allow a counter to be reset in the presence of a persistent error, while preventing specific information, such as that identifying a FRU, from being lost if an error is detected while the previous error is being logged.

Component	Offset	Instance	Range
RAS	0x030 + (64 * n)	ERR<n>MISC2	None

This interface is accessible as follows:

RW

B.1.2.1.7 ERR<n>MISC3, Error Record <n> Miscellaneous Register 3, n = 0 - 9

Reserved error syndrome register.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

RAS

Register offset

$0x038 + (64 * n)$

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-12: EXT\_ERR<n>MISC3 bit assignments

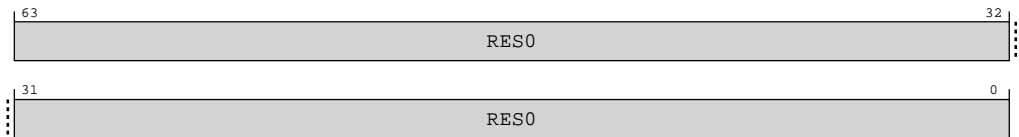


Table B-25: ERR<n>MISC3 bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Access

Arm recommends that a miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.

When ext-ERR<n>STATUS.MV is set to 1, the miscellaneous syndrome for the most recently recorded error should ignore writes.

Accessibility

Arm recommends that a miscellaneous syndrome for multiple errors, such as a corrected error counter, is read/write.

When ext-ERR<n>STATUS.MV is set to 1, the miscellaneous syndrome for the most recently recorded error should ignore writes.

Component	Offset	Instance	Range
RAS	0x038 + (64 * n)	ERR<n>MISC3	None

This interface is accessible as follows:

RW

B.1.2.1.8 ERR<n>PFGF, Error Record <n> Pseudo-fault Generation Feature Register, n = 0 - 9

Defines which common architecturally-defined fault generation features are implemented.

Configurations

Present only when error record <n> is implemented, and error record <n> is the first error record owned by a node. Otherwise, RES0.

ext-ERR<n>FR describes the features implemented by the node.

Attributes

Width

64

Component

RAS

Register offset

0x800 + (64 \* n)

Access type

RO

Reset value

When n == 1, or n == 4, or n == 7 or n == 8

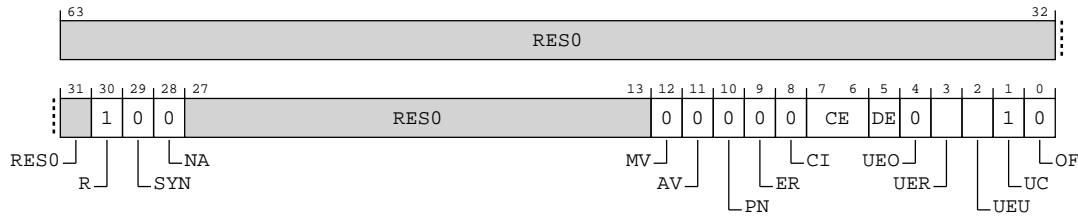
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx x100 xxxx xxxx xxxx xxx0 0000 xxx0 xx10  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When n == 1, or n == 4, or n == 7 or n == 8

**Figure B-13: EXT\_ERR<n>PFGF bit assignments****Table B-27: ERR<n>PFGF bit descriptions**

Bits	Name	Description	Reset
[63:31]	RES0	Reserved	RES0
[30]	R	Restartable. Support for Error Generation Counter restart mode. <b>0b1</b> Error Generation Counter restart mode is implemented and is controlled by ext-ERR<n>PFGCTL.R. ext-ERR<n>PFGCTL.R is a read/write field.	0b1
[29]	SYN	Syndrome. Fault syndrome injection. <b>0b0</b> When an injected error is recorded, the node sets ext-ERR<n>STATUS.{IERR, SERR} to IMPLEMENTATION DEFINED values. ext-ERR<n>STATUS.{IERR, SERR} are <b>UNKNOWN</b> when ext-ERR<n>STATUS.V is 0. <b>Note:</b> If ERR<n>PFGF.SYN is 1, software can write specific values into the ext-ERR<n>STATUS.{IERR, SERR} fields when setting up a fault injection event. The sets of values that can be written to these fields is <b>IMPLEMENTATION DEFINED</b> .	0b0
[28]	NA	No access required. Defines whether this component fakes detection of the error on an access to the component or spontaneously in the fault injection state. <b>0b0</b> The component fakes detection of the error on an access to the component.	0b0
[27:13]	RES0	Reserved	RES0
[12]	MV	Miscellaneous syndrome. Defines whether software can control all or part of the syndrome recorded in the ERR<n>MISC<m> registers when an injected error is recorded. <b>0b0</b> When an injected error is recorded, the node will record additional syndrome in ERR<n>MISC0 and ext-ERR<n>STATUS.MV will be set to 1. If ERR<n>PFGF.MV is 1, software can write specific additional syndrome values into the ERR<n>MISC<m> registers when setting up a fault injection event. The permitted values that can be written to these registers are <b>IMPLEMENTATION DEFINED</b> .	0b0
[11]	AV	Address syndrome. Address syndrome injection. <b>0b0</b> When an injected error is recorded, the node leaves ext-ERR<n>ADDR unchanged. ext-ERR<n>STATUS.AV is always set to 0.	0b0

Bits	Name	Description	Reset
[10]	PN	<p>Poison flag. Describes how the fault generation feature of the node sets the ext-ERR&lt;n&gt;STATUS.PN status flag.</p> <p><b>0b0</b></p> <p>When an injected error is recorded, the node does not set the ext-ERR&lt;n&gt;STATUS.PN bit. ext-ERR&lt;n&gt;PFGCTL.PN is <b>RES0</b>.</p> <p>This behavior replaces the architecture-defined rules for setting the ext-ERR&lt;n&gt;STATUS.PN bit.</p>	0b0
[9]	ER	<p>Error Reported flag. Describes how the fault generation feature of the node sets the ext-ERR&lt;n&gt;STATUS.ER status flag.</p> <p><b>0b0</b></p> <p>When an injected error is recorded, the node sets ext-ERR&lt;n&gt;STATUS.ER according to the architecture-defined rules for setting the ER field. ext-ERR&lt;n&gt;PFGCTL.ER is <b>RES0</b>.</p>	0b0
[8]	CI	<p>Critical Error flag. Describes how the fault generation feature of the node sets the ext-ERR&lt;n&gt;STATUS.CI status flag.</p> <p><b>0b0</b></p> <p>When an injected error is recorded with ext-ERR&lt;n&gt;PFGCTL.UC == 0b1, the node sets ext-ERR&lt;n&gt;STATUS.CI to 1 in the following cases:</p> <ul style="list-style-type: none"> <li>• When a snoop request is received by the L1 D-cache.</li> <li>• When L2 cache is accessed.</li> </ul> <p>This behavior replaces the architecture-defined rules for setting the ext-ERR&lt;n&gt;STATUS.CI bit. ext-ERR&lt;n&gt;PFGCTL.CI is <b>RES0</b>.</p>	0b0
[7:6]	CE	<p><b>When n == 1 or n == 4</b></p> <p>Corrected Error generation. Describes the types of Corrected Error that the fault generation feature of the node can generate.</p> <p><b>01</b></p> <p>The fault generation feature of the node allows generation of a non-specific Corrected error, that is, a Corrected error that is recorded by setting ext-ERR&lt;n&gt;STATUS.CE to 0b10. ext-ERR&lt;n&gt;PFGCTL.CE is a read/write field. The values 0b10 and 0b11 in ext-ERR&lt;n&gt;PFGCTL.CE are reserved.</p> <p><b>When n == 7 or n == 8</b></p> <p>Corrected Error generation. Describes the types of Corrected Error that the fault generation feature of the node can generate.</p> <p><b>00</b></p> <p>The fault generation feature of the node does not generate Corrected errors. ext-ERR&lt;n&gt;PFGCTL.CE is <b>RES0</b>.</p> <p><b>Otherwise</b></p> <p><b>RES0</b></p>	xx

Bits	Name	Description	Reset
[5]	DE	<p><b>When n == 1 or n == 4</b></p> <p>Deferred Error generation. Describes whether the fault generation feature of the node can generate Deferred errors.</p> <p><b>1</b></p> <p>The fault generation feature of the node allows generation of Deferred errors. ext-ERR&lt;n&gt;PFGCTL.DE is a read/write field.</p> <p><b>Otherwise</b></p> <p>Deferred Error generation. Describes whether the fault generation feature of the node can generate Deferred errors.</p> <p><b>0</b></p> <p>The fault generation feature of the node does not generate Deferred errors. ext-ERR&lt;n&gt;PFGCTL.DE is RES0.</p>	x
[4]	UEO	<p>Latent or Restartable Error generation. Describes whether the fault generation feature of the node can generate Latent or Restartable errors.</p> <p><b>0b0</b></p> <p>The fault generation feature of the node does not generate Latent or Restartable errors. ext-ERR&lt;n&gt;PFGCTL.UEO is <b>RES0</b>.</p>	0b0
[3]	UER	<p><b>When n == 7</b></p> <p>Signaled or Recoverable Error generation. Describes whether the fault generation feature of the node can generate Signaled or Recoverable errors.</p> <p><b>1</b></p> <p>The fault generation feature of the node allows generation of Signaled or Recoverable errors. ext-ERR&lt;n&gt;PFGCTL.UER is a read/write field.</p> <p><b>Otherwise</b></p> <p>Signaled or Recoverable Error generation. Describes whether the fault generation feature of the node can generate Signaled or Recoverable errors.</p> <p><b>0</b></p> <p>The fault generation feature of the node does not generate Signaled or Recoverable errors. ext-ERR&lt;n&gt;PFGCTL.UER is RES0.</p>	x
[2]	UEU	<p><b>When n == 4</b></p> <p>Unrecoverable Error generation. Describes whether the fault generation feature of the node can generate Unrecoverable errors.</p> <p><b>1</b></p> <p>The fault generation feature of the node allows generation of Unrecoverable errors. ext-ERR&lt;n&gt;PFGCTL.UEU is a read/write field.</p> <p><b>Otherwise</b></p> <p>Unrecoverable Error generation. Describes whether the fault generation feature of the node can generate Unrecoverable errors.</p> <p><b>0</b></p> <p>The fault generation feature of the node does not generate Unrecoverable errors. ext-ERR&lt;n&gt;PFGCTL.UEU is RES0.</p>	x

Bits	Name	Description	Reset
[1]	UC	Uncontainable Error generation. Describes whether the fault generation feature of the node can generate Uncontainable errors.  <b>0b1</b>  The fault generation feature of the node allows generation of Uncontainable errors. ext-ERR<n>PFGCTL.UC is a read/write field.	0b1
[0]	OF	Overflow flag. Describes how the fault generation feature of the node sets the ext-ERR<n>STATUS.OF status flag.  <b>0b0</b>  When an injected error is recorded, the node sets ext-ERR<n>STATUS.OF according to the architecture-defined rules for setting the OF field. ext-ERR<n>PFGCTL.OF is <b>RES0</b> .	0b0

Figure B-14: EXT\_ERR<n>PFGF bit assignments

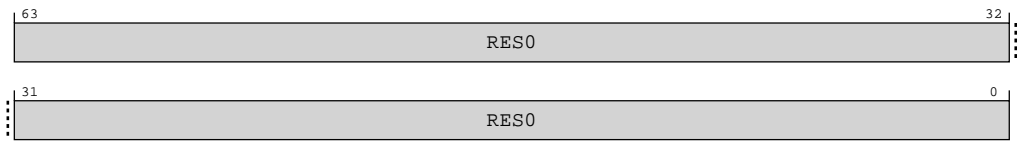


Table B-28: ERR<n>PFGF bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
RAS	0x800 + (64 * n)	ERR<n>PFGF	None

This interface is accessible as follows:

RO

B.1.2.1.9 ERR<n>PFGCTL, Error Record <n> Pseudo-fault Generation Control Register, n = 0 - 9

Enables controlled fault generation.

Configurations

Present only when error record <n> is implemented, and error record <n> is the first error record owned by a node. Otherwise, RES0.

ext-ERR<n>FR describes the features implemented by the node.

Attributes

Width

64



Component

RAS

Register offset

0x808 + (64 \* n)

Access type

RW

Reset value

When n == 1, or n == 4, or n == 7 or n == 8

xxxx xxxx xxxx xxxx xxxx xxxx xxxx 0xxx xxxx xxxx xxx1 xxxx xxxx xxxx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When n == 1, or n == 4, or n == 7 or n == 8

Figure B-15: EXT\_ERR<n>PFGCTL bit assignments

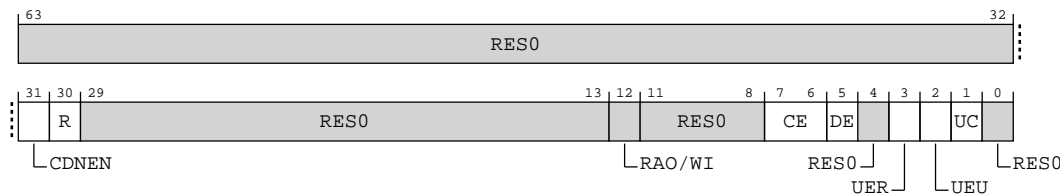


Table B-30: ERR<n>PFGCTL bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	CDNEN	Countdown Enable. Controls transfers of the value held in ext-ERR<n>PFGCDN to the Error Generation Counter and enables this counter.  <b>0b0</b> The Error Generation Counter is disabled.  <b>0b1</b> The Error Generation Counter is enabled. On a write of 1 to this field, the Error Generation Counter is set to ext-ERR<n>PFGCDN.CDN.	0b0

Bits	Name	Description	Reset
[30]	R	<p>Restart. Controls whether, on reaching zero, the Error Generation Counter restarts from the ext-ERR&lt;n&gt;PFGCDN value, or stops.</p> <p><b>0b0</b></p> <p>On reaching 0, the Error Generation Counter stops.</p> <p><b>0b1</b></p> <p>On reaching 0, the Error Generation Counter is set to ext-ERR&lt;n&gt;PFGCDN.CDN.</p>	x
[29:13]	RES0	Reserved	RES0
[12]	RAO/WI	Reserved	RAO/ WI
[11:8]	RES0	Reserved	RES0
[7:6]	CE	<p><b>When n == 1 or n == 4</b></p> <p>Corrected Error generation enable. Controls the type of injected Corrected error generated by the fault injection feature of the node.</p> <p><b>0b00</b></p> <p>An injected Corrected error will not be generated by the fault injection feature of the node.</p> <p><b>0b01</b></p> <p>An injected non-specific Corrected error is generated in the fault injection state. ext-ERR&lt;n&gt;STATUS.CE is set to 0b10 when the injected error is recorded.</p> <p>The set of permitted values for this field is defined by ext-ERR&lt;n&gt;PFGF.CE.</p> <p>The node enters the fault injection state when the Error Generation Counter decrements to zero. The injected error is not generated when the error is generated on an access to the component in the fault injection state and the data is not consumed.</p> <p><b>Otherwise</b></p> <p>RES0</p>	xx
[5]	DE	<p><b>When n == 1 or n == 4</b></p> <p>Deferred Error generation enable. Controls whether an injected Deferred error is generated by the fault injection feature of the node.</p> <p><b>0b0</b></p> <p>An injected Deferred error will not be generated by the fault generation feature of the node.</p> <p><b>0b1</b></p> <p>An injected Deferred error is generated in the fault injection state.</p> <p>The node enters the fault injection state when the Error Generation Counter decrements to zero. The injected error is not generated when the error is generated on an access to the component in the fault injection state and the data is not consumed.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3]	UER	<p><b>When n == 7</b></p> <p>Signaled or Recoverable Error generation enable. Controls whether an injected Signaled or Recoverable error is generated by the fault injection feature of the node.</p> <p><b>0b0</b></p> <p>An injected Signaled or Recoverable error will not be generated by the fault generation feature of the node.</p> <p><b>0b1</b></p> <p>An injected Signaled or Recoverable error is generated in the fault injection state.</p> <p>The node enters the fault injection state when the Error Generation Counter decrements to zero.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[2]	UEU	<p><b>When n == 4</b></p> <p>Unrecoverable Error generation enable. Controls whether an injected Unrecoverable error is generated by the fault injection feature of the node.</p> <p><b>0b0</b></p> <p>An injected Unrecoverable error will not be generated by the fault generation feature of the node.</p> <p><b>0b1</b></p> <p>An injected Unrecoverable error is generated in the fault injection state.</p> <p>The node enters the fault injection state when the Error Generation Counter decrements to zero. The injected error is not generated when the error is generated on an access to the component in the fault injection state and the data is not consumed.</p> <p>If AArch64-IMP_CLUSTERACTLR_EL1.L2EC is zero, an Unrecoverable Error cannot be generated at node 4.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[1]	UC	<p>Uncontainable Error generation enable. Controls whether an injected Uncontainable error is generated by the fault injection feature of the node.</p> <p><b>0b0</b></p> <p>An injected Uncontainable error will not be generated by the fault generation feature of the node.</p> <p><b>0b1</b></p> <p>An injected Uncontainable error is generated in the fault injection state.</p> <p>The node enters the fault injection state when the Error Generation Counter decrements to zero. The injected error is not generated when the error is generated on an access to the component in the fault injection state and the data is not consumed.</p> <p>If AArch64-IMP_CLUSTERACTLR_EL1.L2EC is one, an Uncontainable Error cannot be generated at node 4.</p>	x
[0]	RES0	Reserved	RES0

Figure B-16: EXT\_ERR<n>PFGCTL bit assignments

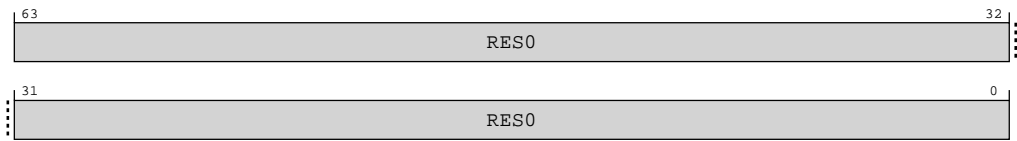


Table B-31: ERR<n>PFGCTL bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
RAS	0x808 + (64 * n)	ERR<n>PFGCTL	None

This interface is accessible as follows:

RW

B.1.2.1.10 ERR<n>PFGCDN, Error Record <n> Pseudo-fault Generation Countdown Register, n = 0 - 9

Generates one of the errors enabled in the corresponding ext-ERR<n>PFGCTL register.

Configurations

ext-ERR<n>FR describes the features implemented by the node.

This register is present only when n == 1, or n == 4 or (n == 7 or n == 8). Otherwise, direct accesses to ERR<n>PFGCDN are UNDEFINED.

Attributes

Width

64

Component

RAS

Register offset

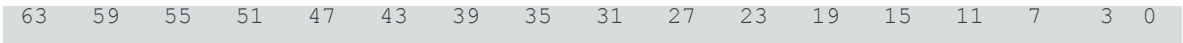
0x810 + (64 \* n)

Access type

RW

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-17: EXT\_ERR<n>PFGCDN bit assignments

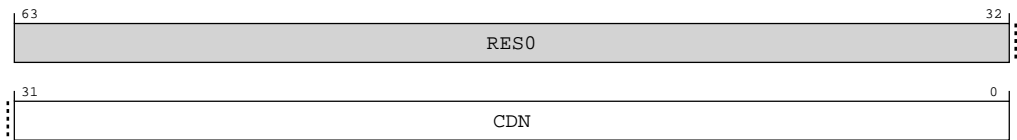


Table B-33: ERR<n>PFGCDN bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	CDN	Countdown value.  This field is copied to Error Generation Counter when either: <ul style="list-style-type: none"><li>Software writes 1 to ext-ERR&lt;n&gt;PFGCTL.CDNEN.</li><li>The Error Generation Counter decrements to zero and ext-ERR&lt;n&gt;PFGCTL.R is 1.</li></ul> While ext-ERR<n>PFGCTL.CDNEN is 1 and the Error Generation Counter is nonzero, the counter decrements by 1 for each cycle at the core clock rate. When the counter reaches zero, one of the errors enabled in the ext-ERR<n>PFGCTL register is generated.  <b>Note:</b> The current Error Generation Counter value is not visible to software.	32 {x}

Accessibility

Component	Offset	Instance	Range
RAS	0x810 + (64 * n)	ERR<n>PFGCDN	None

This interface is accessible as follows:

RW

B.1.2.1.11 ERRGSR, Error Group Status Register

Shows the status for the records in the group.

Configurations

If an error record is not implemented, the corresponding bit in this register will read as 0.

Attributes

Width

64

Component

RAS

Register offset

0xE00

Access type

RO

Reset value

xxxx	xxxx	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	00xx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-18: EXT\_ERRGSR bit assignments

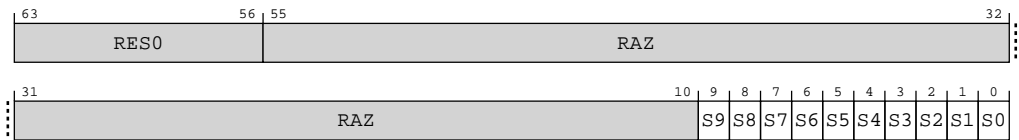


Table B-35: ERRGSR bit descriptions

Bits	Name	Description	Reset
[63:56]	RES0	Reserved	RES0
[55:10]	RAZ	Reserved	RAZ

Bits	Name	Description	Reset
[9]	S9	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more errors detected from the cluster by the safety mechanisms. See ext-ERR9STATUS.V.</p>	x
[8]	S8	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more errors detected from the cluster by the safety mechanisms. See ext-ERR8STATUS.V.</p>	x
[7]	S7	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more errors detected from the cores by the safety mechanisms. See ext-ERR7STATUS.V.</p>	x
[6]	S6	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more memory ECC errors from L2 cache or LCU. See ext-ERR6STATUS.V.</p>	x
[5]	S5	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more memory ECC errors from L2 cache or LCU. See ext-ERR5STATUS.V.</p>	x
[4]	S4	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more memory ECC errors from L2 cache or LCU. See ext-ERR4STATUS.V.</p>	x
[3]	S3	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more memory ECC errors from L1 I-cache, L1 D-cache, ITCM, DTCM or MMS. See ext-ERR3STATUS.V.</p>	x
[2]	S2	<p>The status for error record &lt;m&gt;. A read-only copy of ERR&lt;m&gt;STATUS.V.</p> <p><b>0b0</b> No error.</p> <p><b>0b1</b> One or more memory ECC errors from L1 I-cache, L1 D-cache, ITCM, DTCM or MMS. See ext-ERR2STATUS.V.</p>	x

Bits	Name	Description	Reset
[1]	S1	The status for error record <m>. A read-only copy of ERR<m>STATUS.V.  <b>0b0</b> No error.  <b>0b1</b> One or more memory ECC errors from L1 I-cache, L1 D-cache, ITCM, DTCM or MMS. See ext-ERR1STATUS.V.	x
[0]	S0	The status for error record <m>. A read-only copy of ERR<m>STATUS.V.  <b>0b0</b> No error.  <b>0b1</b> One or more memory non-ECC errors from L2 cache or LCU. See ext-ERR0STATUS.V.	x

Accessibility

Component	Offset	Instance	Range
RAS	0xE00	ERRGSR	None

This interface is accessible as follows:

RO

B.1.2.1.12   ERRIIDR, Implementation Identification Register

Defines the implementer of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

RAS

Register offset

0xE10

Access type

RO

Reset value

1101	0001	0100	0111	xxxx	0100	x011	1011
31	27	23	19	15	11	7	3 0

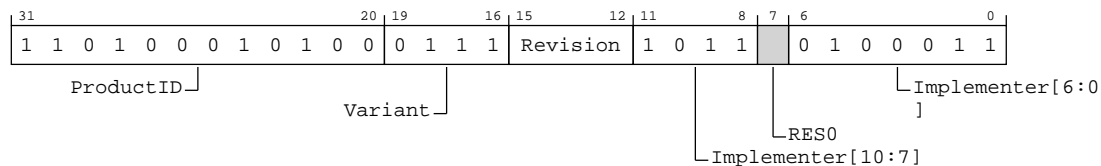


**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-19: EXT\_ERRIIDR bit assignments**



**Table B-37: ERRIIDR bit descriptions**

Bits	Name	Description	Reset
[31:20]	ProductID	Part number.  <b>0b110100010100</b> Cortex-R82AE RAS component.	0xD14
[19:16]	Variant	Component major revision.  <b>0b0111</b> Product revision 7.	0b0111
[15:12]	Revision	Component minor revision.  <b>0b0000</b> No ECO fixes.	xxxx
[11:8, 6:0]	Implementer	Contains the JEP106 code of the company that implemented the RAS component.  <b>0b01000111011</b> Arm Limited.  Bits [11:8] contain the JEP106 continuation code of the implementer, and bits [6:0] contain the JEP106 identity code of the implementer.  ext-ERRPIDR4.DES_2 matches bits [11:8] of ERRIIDR.Implementer, ext-ERRPIDR2.DES_1 matches bits [6:4] of ERRIIDR.Implementer, and ext-ERRPIDR1.DES_0 matches bits [3:0] of ERRIIDR.Implementer.	0b01000111011
[7]	RES0	Reserved	RES0

## Accessibility

Component	Offset	Range
RAS	0xE10	None

This interface is accessible as follows:

RO

B.1.2.1.13 ERRDEVAFF, Device Affinity Register

The processor records have mixed affinity, and so this register is not implemented.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

RAS

Register offset

0xFA8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-20: EXT\_ERRDEVAFF bit assignments

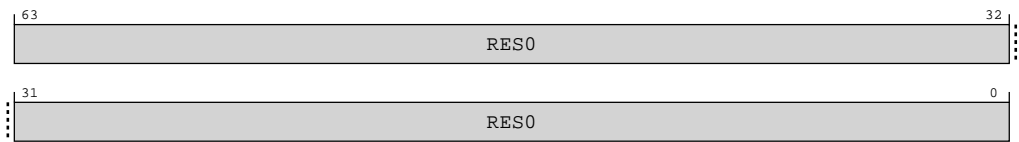


Table B-39: ERRDEVAFF bit descriptions

Bits	Name	Description	Reset
[63:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
RAS	0xFA8	ERRDEVAFF	None

This interface is accessible as follows:

RO

B.1.2.1.14 ERRDEVARCH, Device Architecture Register

Provides discovery information for the component.

Configurations

ERRDEVARCH is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFBC

Access type

RO

Reset value

0100 0111 0111 0001 0000 1010 0000 0000

Bit descriptions

Figure B-21: EXT\_ERRDEVARCH bit assignments

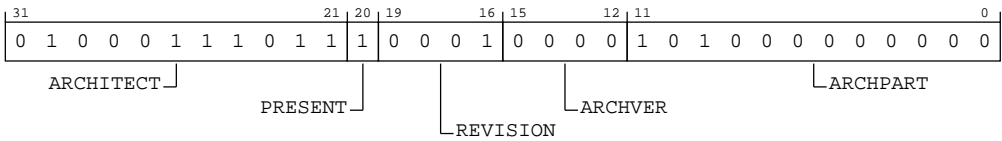


Table B-41: ERRDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect. Defines the architect of the component. Bits [31:28] are the JEP106 continuation code (JEP106 bank ID, minus 1) and bits [27:21] are the JEP106 ID code.  <b>0b01000111011</b> JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	DEVARCH present. Defines that ERRDEVARCH register is present. Defined values are:  <b>0b1</b> Device Architecture information present.  This field reads as 1.	0b1

Bits	Name	Description	Reset
[19:16]	REVISION	Revision. Defines the architecture revision of the component. Defined values are:  <b>0b0001</b> RAS System Architecture, error record group v1.1. As 0b0000 and also: <ul style="list-style-type: none"> <li>• Simplifies ext-ERR&lt;n&gt;STATUS.</li> <li>• Adds support for additional ERR&lt;n&gt;MISC&lt;m&gt; registers.</li> <li>• Adds support for the optional RAS Timestamp Extension.</li> <li>• Adds support for the optional Common Fault Injection Model Extension.</li> </ul> All other values are reserved.	0b0001
[15:12]	ARCHVER	Architecture Version. Defines the architecture version of the component. Defined values are:  <b>0b0000</b> RAS System Architecture, error record group v1.  All other values are reserved.  ERRDEVARCH.ARCHVER and ERRDEVARCH.ARCHPART are also defined as a single field, ERRDEVARCH.ARCHID, so that ERRDEVARCH.ARCHVER is ERRDEVARCH.ARCHID[15:12].	0b0000
[11:0]	ARCHPART	Architecture Part. Defines the architecture of the component. Defined values are:  <b>0b101000000000</b> RAS System Architecture, error record group.  ERRDEVARCH.ARCHVER and ERRDEVARCH.ARCHPART are also defined as a single field, ERRDEVARCH.ARCHID, so that ERRDEVARCH.ARCHPART is ERRDEVARCH.ARCHID[11:0].	0xA00

## Accessibility

Component	Offset	Instance	Range
RAS	0xFBC	ERRDEVARCH	None

This interface is accessible as follows:

RO

### B.1.2.1.15 ERRDEVID, Device Configuration Register

Provides discovery information for the component.

## Configurations

ERRDEVID is implemented only as part of a memory-mapped group of error records.

## Attributes

### Width

32

### Component

RAS

Register offset

0xFC8

Access type

RO

Reset value

xxxx	xxxx	xx0x	0000	0000	0000	0000	1010
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-22: EXT\_ERRDEVID bit assignments

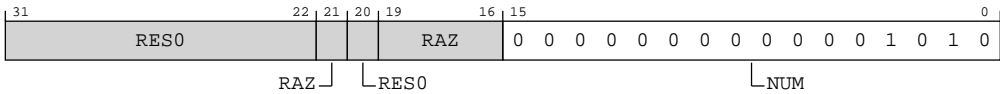


Table B-43: ERRDEVID bit descriptions

Bits	Name	Description	Reset
[31:22]	RES0	Reserved	RES0
[21]	RAZ	Reserved	RAZ
[20]	RES0	Reserved	RES0
[19:16]	RAZ	Reserved	RAZ
[15:0]	NUM	Highest numbered index of the records that can be accessed through the Error Record System registers plus one.  0b00000000000001010 10 error records implemented.	0x000A

Accessibility

Component	Offset	Instance	Range
RAS	0xFC8	ERRDEVID	None

This interface is accessible as follows:

RO

B.1.2.1.16    ERRPIDR4, Peripheral Identification Register 4

Provides discovery information about the component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRPIDR4 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFD0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-23: EXT\_ERRPIDR4 bit assignments

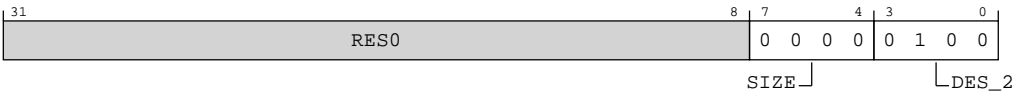


Table B-45: ERRPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	Size of the component. <b>RAZ</b> . Log <sub>2</sub> of the number of 4KB pages from the start of the component to the end of the component ID registers.  <b>0b0000</b> The component uses a single 4KB block.	0b0000

Bits	Name	Description	Reset
[3:0]	DES_2	Designer, JEP106 continuation code, least significant nibble. For Arm Limited, this field is 0b0100.  <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Instance	Range
RAS	0xFD0	ERRPIDR4	None

This interface is accessible as follows:

RO

B.1.2.1.17 ERRPIDR0, Peripheral Identification Register 0

Provides discovery information about the component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRPIDR0 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFE0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0100
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-24: EXT\_ERRPIDR0 bit assignments

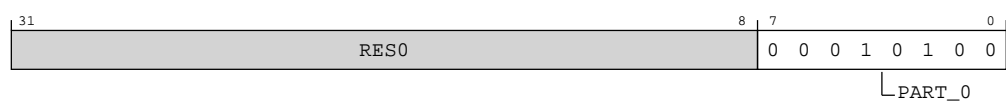


Table B-47: ERRPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0]. <b>0b00010100</b> Cortex-R82AE RAS component. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Instance	Range
RAS	0xFE0	ERRPIDR0	None

This interface is accessible as follows:

RO

B.1.2.1.18 ERRPIDR1, Peripheral Identification Register 1

Provides discovery information about the component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRPIDR1 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFE4

Access type

RO



Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-25: EXT\_ERRPIDR1 bit assignments

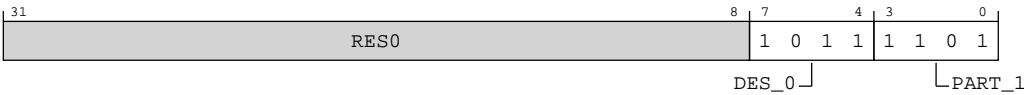


Table B-49: ERRPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	Designer, least significant nibble of JEP106 ID code. For Arm Limited, this field is 0b1011.  0b1011 Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8].  0b1101 Cortex-R82AE RAS component. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Instance	Range
RAS	0xFE4	ERRPIDR1	None

This interface is accessible as follows:

RO

B.1.2.1.19 ERRPIDR2, Peripheral Identification Register 2

Provides discovery information about the component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRPIDR2 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFE8

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-26: EXT\_ERRPIDR2 bit assignments

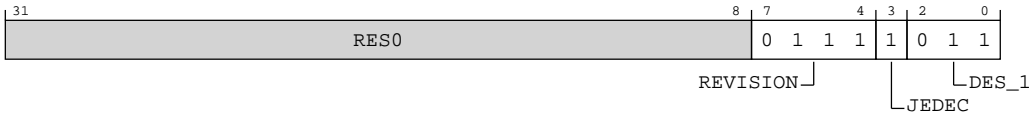


Table B-51: ERRPIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Instance	Range
RAS	0xFE8	ERRPIDR2	None

This interface is accessible as follows:

RO

B.1.2.1.20 ERRPIDR3, Peripheral Identification Register 3

Provides discovery information about the component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRPIDR3 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFEC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-27: EXT\_ERRPIDR3 bit assignments

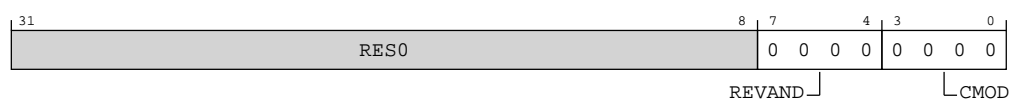


Table B-53: ERRPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Part minor revision. Parts using ext-ERRPIDR2.REVISION as an extension to the Part number must use this field as a major revision number.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer modified. Indicates someone other than the Designer has modified the component.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Instance	Range
RAS	0xFEC	ERRPIDR3	None

This interface is accessible as follows:

RO

B.1.2.1.21 ERRCIDR0, Component Identification Register 0

Provides discovery information about the component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRCIDR0 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

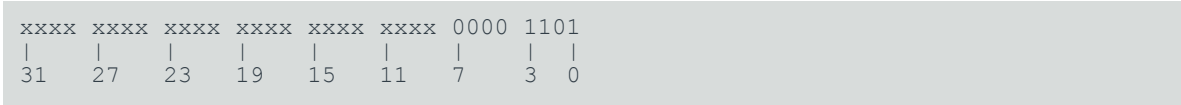
RAS

Register offset

0xFF0

Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-28: EXT\_ERRCIDR0 bit assignments



Table B-55: ERRCIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble. <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Instance	Range
RAS	0xFF0	ERRCIDR0	None

This interface is accessible as follows:

RO

B.1.2.1.22 ERRCIDR1, Component Identification Register 1

Provides discovery information about the component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRCIDR1 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFF4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-29: EXT\_ERRCIDR1 bit assignments



Table B-57: ERRCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	Component class. <b>0b1111</b> Generic peripheral with <b>IMPLEMENTATION DEFINED</b> register layout.  Other values are defined by the CoreSight Architecture.  This field reads as 0xF.	0b1111
[3:0]	PRMBL_1	Preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Instance	Range
RAS	0xFF4	ERRCIDR1	None

This interface is accessible as follows:

RO

B.1.2.1.23   ERRCIDR2, Component Identification Register 2

Provides discovery information about the component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRCIDR2 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFF8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-30: EXT\_ERRCIDR2 bit assignments

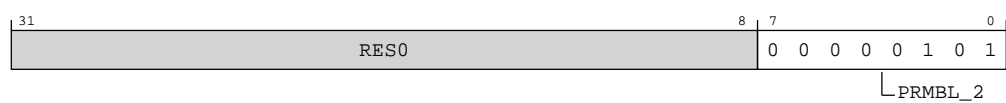


Table B-59: ERRCIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble. <b>0b00000101</b> CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Instance	Range
RAS	0xFF8	ERRCIDR2	None

This interface is accessible as follows:

RO

B.1.2.1.24 ERRCIDR3, Component Identification Register 3

Provides discovery information about the component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

ERRCIDR3 is implemented only as part of a memory-mapped group of error records.

Attributes

Width

32

Component

RAS

Register offset

0xFFC

Access type

RO



Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-31: EXT\_ERRCIDR3 bit assignments



Table B-61: ERRCIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble.  0b10110001 CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Instance	Range
RAS	0xFFC	ERRCIDR3	None

This interface is accessible as follows:

RO

B.1.2.2 External PPU register description

This section includes the register descriptions for all memory-mapped *Power Policy Unit* (PPU) registers that are accessed for each core in the Cortex®-R82AE processor.

B.1.2.2.1 PPU\_PWPR, Power Policy Register

This register enables software to program both power and operating mode policy. It also contains related settings including the enable for dynamic transitions and the lock enable.

This register does not reflect the current power mode value. The current power mode of the domain is reflected in the Power Status Register (ext-PPU\_PWSR).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x000

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-32: EXT\_PPU\_PWPR bit assignments

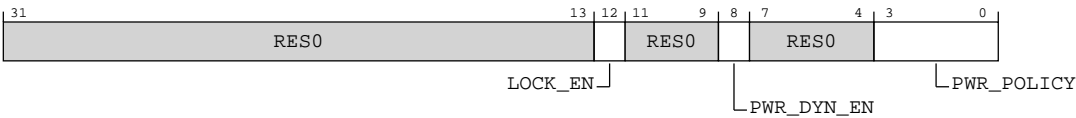


Table B-63: PPU\_PWPR bit descriptions

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[12]	LOCK_EN	Lock enable bit.  <b>0b0</b> Lock feature disabled.  <b>0b1</b> Lock feature enabled.	0b0
[11:9]	RES0	Reserved	RES0
[8]	PWR_DYN_EN	Power mode dynamic transition enable.  <b>0b0</b> Dynamic transitions disabled for power modes.  <b>0b1</b> Dynamic transitions enabled for power modes, allowing transitions to be initiated by changes on power mode DEVACTIVE inputs.	0b1
[7:4]	RES0	Reserved	RES0
[3:0]	PWR_POLICY	Power mode policy.  When static power mode transitions are enabled, PWR_DYN_EN is set to 0b0, this is the target power mode for the PPU.  When dynamic power mode transitions are enabled, PWR_DYN_EN is set to 0b1, this is the minimum power mode for the PPU.  <b>0b0000</b> OFF. Logic off and RAM off.  <b>0b0001</b> OFF_EMU. Emulated Off. Logic on with RAM on. This mode is used to emulate the functional condition of OFF without removing power.  <b>0b0101</b> FULL_RET. Full Retention. Logic and RAM in retention.  <b>0b0111</b> FUNC_RET. Functional Retention. Floating-point/Vector logic retained, rest of the core logic and RAM on, core is functional.  <b>0b1000</b> ON. Logic on with RAM on, core is functional.  <b>0b1001</b> WARM_RST. Warm Reset. Warm reset application with logic and RAM on.  <b>0b1010</b> DBG_RECOV. Debug Recovery Reset. Warm reset application with logic and RAM on.	0b0000

## Accessibility

Component	Offset	Range
PPU	0x000	None

This interface is accessible as follows:

RW

B.1.2.2.2 PPU\_PMER, Power Mode Emulation Enable Register

This register allows software to enable entry into emulated modes.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

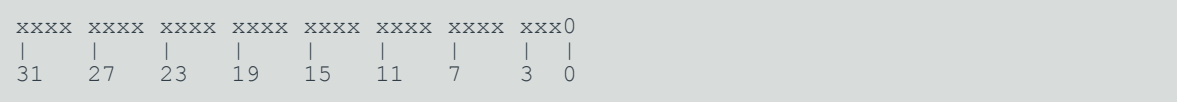
Register offset

0x004

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-33: EXT\_PPU\_PMER bit assignments

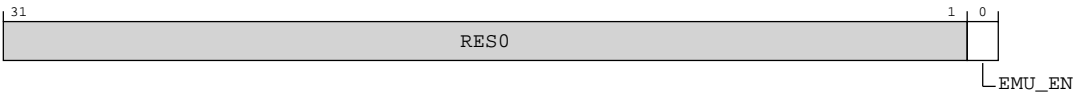


Table B-65: PPU\_PMER bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	EMU_EN	Power mode emulation enable.  <b>0b0</b> Power mode emulation disabled.  <b>0b1</b> Power mode emulation enabled. Transitions to OFF and MEM_RET instead transition to OFF_EMU and MEM_RET_EMU.	0b0

Accessibility

Component	Offset	Range
PPU	0x004	None

This interface is accessible as follows:

RW

B.1.2.2.3 PPU\_PWSR, Power Status Register

This read-only register contains status information for the power mode, operating mode, dynamic transitions, and lock feature.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x008

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxx0	xxx1	xxxx	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-34: EXT\_PPU\_PWSR bit assignments

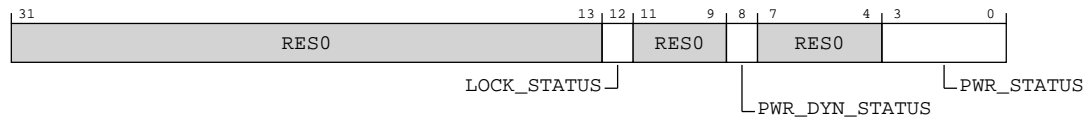


Table B-67: PPU\_PWSR bit descriptions

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0
[12]	LOCK_STATUS	Lock status.  <b>0b0</b> The PPU is not locked in the current mode.  <b>0b1</b> The PPU is locked in the current mode.	0b0
[11:9]	RES0	Reserved	RES0
[8]	PWR_DYN_STATUS	Power mode dynamic transition status.  There might be a delay in dynamic transitions becoming active or inactive if the PPU is transitioning when ext-PPU_PWPR.DYN_EN is programmed.  <b>0b0</b> Dynamic transitions disabled for power modes.  <b>0b1</b> Dynamic transitions enabled for power modes.	0b1
[7:4]	RES0	Reserved	RES0
[3:0]	PWR_STATUS	Power mode status.  These bits reflect the current power mode of the PPU.  <b>0b0000</b> OFF. Logic off and RAM off.  <b>0b0001</b> OFF_EMU. Emulated Off. Logic on with RAM on. This mode is used to emulate the functional condition of OFF without removing power.  <b>0b0101</b> FULL_RET. Full Retention. Logic and RAM in retention.  <b>0b0111</b> FUNC_RET. Functional Retention. Floating-point/Vector logic retained, rest of the core logic and RAM on, core is functional.  <b>0b1000</b> ON. Logic on with RAM on, core is functional.  <b>0b1001</b> WARM_RST. Warm Reset. Warm reset application with logic and RAM on.  <b>0b1010</b> DBG_RECOV. Debug Recovery Reset. Warm reset application with logic and RAM on.	0b0000

Accessibility

Component	Offset	Range
PPU	0x008	None

This interface is accessible as follows:

RO

B.1.2.2.4 PPU\_DISR, Device Interface Input Current Status Register

This read-only register contains status reflecting the values of the device interface inputs.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x010

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	x000	0000	0000
31	27	23	19	15	11	7	3 0

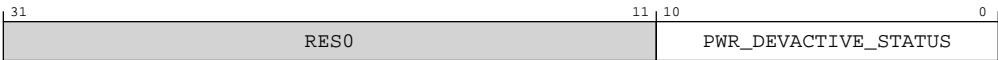


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-35: EXT\_PPU\_DISR bit assignments



**Table B-69: PPU\_DISR bit descriptions**

Bits	Name	Description	Reset
[31:11]	RES0	Reserved	RES0
[10:0]	PWR_DEVACTIVE_STATUS	<p>Status of the power mode DEVPACTIVE inputs.</p> <p><b>0b000000000000</b> Request for OFF.</p> <p><b>0000000001x</b> Request for OFF_EMU.</p> <p><b>000001xxxxx</b> Request for FULL_RET.</p> <p><b>0001xxxxxxx</b> Request for FUNC_RET.</p> <p><b>001xxxxxxxx</b> Request for ON.</p> <p><b>01xxxxxxxxx</b> Request for WARM_RST.</p> <p><b>1xxxxxxxxxx</b> Request for DBG_RECOV.</p>	0b000000000000

### Accessibility

Component	Offset	Range
PPU	0x010	None

This interface is accessible as follows:

RO

#### B.1.2.2.5 PPU\_MISR, Miscellaneous Input Current Status Register

This read-only register contains status reflecting the values of miscellaneous inputs.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

PPU

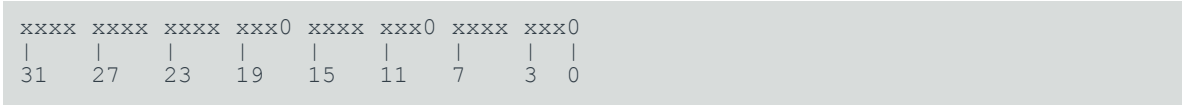
#### Register offset

0x014



Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-36: EXT\_PPU\_MISR bit assignments

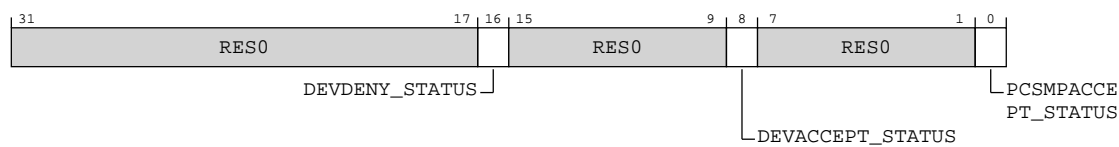


Table B-71: PPU\_MISR bit descriptions

Bits	Name	Description	Reset
[31:17]	RES0	Reserved	RES0
[16]	DEVDPENY_STATUS	Status of the device interface DEVDPENY inputs.  0b0 DEVDPENY deasserted.  0b1 DEVDPENY asserted.	0b0
[15:9]	RES0	Reserved	RES0
[8]	DEVACCEPT_STATUS	Status of the device interface DEVACCEPT inputs.  0b0 DEVACCEPT deasserted.  0b1 DEVACCEPT asserted.	0b0
[7:1]	RES0	Reserved	RES0
[0]	PCSMPACCEPT_STATUS	Status of the PCSMPACCEPT inputs.  0b0 PCSMPACCEPT deasserted.  0b1 PCSMPACCEPT asserted.	0b0

Accessibility

Component	Offset	Range
PPU	0x014	None

This interface is accessible as follows:

RO

B.1.2.2.6 PPU\_STSR, Stored Status Register

This register is reserved for P-channel PPUs.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

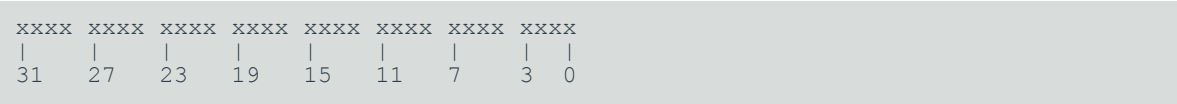
Register offset

0x018

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-37: EXT\_PPU\_STSR bit assignments

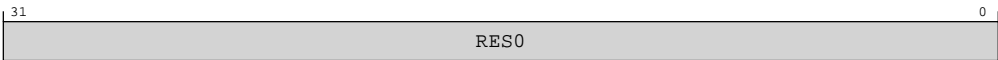


Table B-73: PPU\_STSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x018	None

This interface is accessible as follows:

RO

B.1.2.2.7 PPU\_UNLK, Unlock Register

This register allows software to unlock the PPU from a locked power mode.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x01C

Access type

RAZW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-38: EXT\_PPU\_UNLK bit assignments

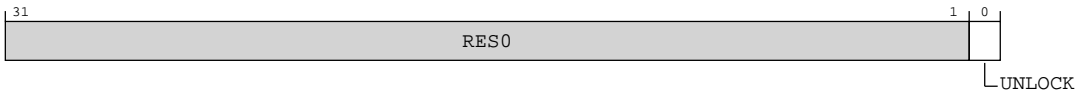


Table B-75: PPU\_UNLK bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	UNLOCK	When 0b1 is written to this bit the PPU is unlocked from a locked power mode. A read always returns 0b0.	0b0

Accessibility


Component	Offset	Range
PPU	0x01C	None

This interface is accessible as follows:

RW

B.1.2.2.8 PPU\_PWCR, Power Configuration Register

This register controls enabling and disabling of hardware control inputs to the PPU.



**Note**

Before software programs the DEVREQEN bits it must configure the PPU for static transitions and ensure the requested power mode has been reached, this means that no further transitions can occur, otherwise behavior is UNPREDICTABLE.

The PWR\_DEVACTIVEEN and OP\_DEVACTIVEEN fields in this register control the ability of the DEVACTIVE inputs to initiate power mode transitions, but not the ability to generate input edge interrupt events.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x020

Access type

RW

Reset value

xxxx	xxxx	xxxx	x111	1111	111x	xxxx	xxx1
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-39: EXT\_PPU\_PWCR bit assignments

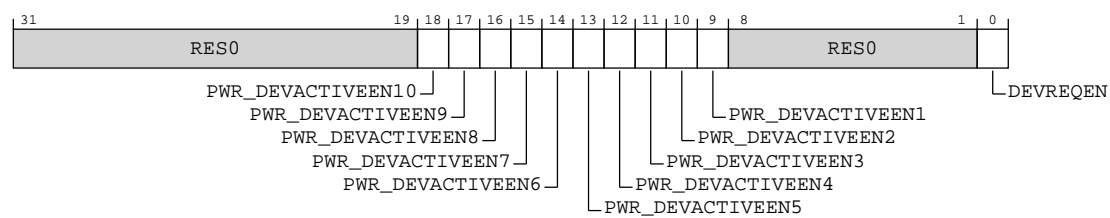


Table B-77: PPU\_PWCR bit descriptions

Bits	Name	Description	Reset
[31:19]	RES0	Reserved	RES0
[18]	PWR_DEVACTIVEEN10	Enables the operating mode DEVPACTIVE[10] input.  <b>0b0</b> DEVPACTIVE[10] input (DBG_RECOV) disabled.  <b>0b1</b> DEVPACTIVE[10] input (DBG_RECOV) enabled.	0b1
[17]	PWR_DEVACTIVEEN9	Enables the operating mode DEVPACTIVE[9] input.  <b>0b0</b> DEVPACTIVE[9] input (WARM_RST) disabled.  <b>0b1</b> DEVPACTIVE[9] input (WARM_RST) enabled.	0b1
[16]	PWR_DEVACTIVEEN8	Enables the operating mode DEVPACTIVE[8] input.  <b>0b0</b> DEVPACTIVE[8] input (ON) disabled.  <b>0b1</b> DEVPACTIVE[8] input (ON) enabled.	0b1

Bits	Name	Description	Reset
[15]	PWR_DEVACTIVEEN7	Enables the operating mode DEVPACTIVE[7] input. <b>0b0</b> DEVPACTIVE[7] input (FUNC_RET) disabled. <b>0b1</b> DEVPACTIVE[7] input (FUNC_RET) enabled.	0b1
[14]	PWR_DEVACTIVEEN6	Enables the operating mode DEVPACTIVE[6] input. <b>0b0</b> DEVPACTIVE[6] input (unused) disabled. <b>0b1</b> DEVPACTIVE[6] input (unused) enabled.	0b1
[13]	PWR_DEVACTIVEEN5	Enables the operating mode DEVPACTIVE[5] input. <b>0b0</b> DEVPACTIVE[5] input (FULL_RET) disabled. <b>0b1</b> DEVPACTIVE[5] input (FULL_RET) enabled.	0b1
[12]	PWR_DEVACTIVEEN4	Enables the operating mode DEVPACTIVE[4] input. <b>0b0</b> DEVPACTIVE[4] input (unused) disabled. <b>0b1</b> DEVPACTIVE[4] input (unused) enabled.	0b1
[11]	PWR_DEVACTIVEEN3	Enables the operating mode DEVPACTIVE[3] input. <b>0b0</b> DEVPACTIVE[3] input (unused) disabled. <b>0b1</b> DEVPACTIVE[3] input (unused) enabled.	0b1
[10]	PWR_DEVACTIVEEN2	Enables the operating mode DEVPACTIVE[2] input. <b>0b0</b> DEVPACTIVE[2] input (unused) disabled. <b>0b1</b> DEVPACTIVE[2] input (unused) enabled.	0b1
[9]	PWR_DEVACTIVEEN1	Enables the operating mode DEVPACTIVE[1] input. <b>0b0</b> DEVPACTIVE[1] input (OFF_EMU) disabled. <b>0b1</b> DEVPACTIVE[1] input (OFF_EMU) enabled.	0b1
[8:1]	<b>RES0</b>	Reserved	<b>RES0</b>
[0]	DEVREQEN	Device interface handshake enable. <b>0b0</b> Device interface handshake disabled for transitions. <b>0b1</b> Device interface handshake enabled for transitions.	0b1

Accessibility

Component	Offset	Range
PPU	0x020	None

This interface is accessible as follows:

RW

B.1.2.2.9 PPU\_PTCR, Power Mode Transition Register

This register contains settings which affect the behaviour of certain power mode transitions.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x024

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx01
31	27	23	19	15	11	7	3 0

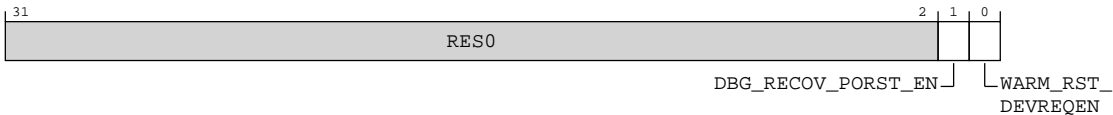


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-40: EXT\_PPU\_PTCR bit assignments



**Table B-79: PPU\_PTCR bit descriptions**

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	DBG_RECOV_PORST_EN	<p>Power-on reset behavior in DBG_RECOV.</p> <p>This bit should not be modified when the PPU is in DBG_RECOV. If it is modified, it will not have any effect on the reset output.</p> <p>This bit should not be modified when the PPU is in transition. If it is modified, the reset output will depend on either the old or the new value of the bit.</p> <p><b>0b0</b></p> <p>DEVPORESETn is not asserted when in DBG_RECOV.</p> <p><b>0b1</b></p> <p>DEVPORESETn is asserted when in DBG_RECOV.</p>	0b0
[0]	WARM_RST_DEVREQEN	<p>Device interface handshake behavior.</p> <p>This bit should not be modified when the PPU is in WARM_RST, or if the PPU is performing a transition, otherwise PPU behavior is <b>UNPREDICTABLE</b>.</p> <p><b>0b0</b></p> <p>The PPU does not perform a device interface handshake when transitioning between ON and WARM_RST.</p> <p><b>0b1</b></p> <p>The PPU performs a device interface handshake when transitioning between ON and WARM_RST.</p>	0b1

### Accessibility

Component	Offset	Range
PPU	0x024	None

This interface is accessible as follows:

RW

#### B.1.2.2.10 PPU\_IMR, Interrupt Mask Register

This register controls the events that assert the interrupt output. Additional event masking controls are in the Additional Interrupt Mask Register (ext-PPU\_AIMR), Input Edge Sensitivity Register (ext-PPU\_IESR), and the Operating Mode Active Edge Sensitivity Register (ext-PPU\_OPSR).

When an interrupt event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

### Configurations

This register is available in all configurations.



Attributes

Width

32

Component

PPU

Register offset

0x030

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-41: EXT\_PPU\_IMR bit assignments

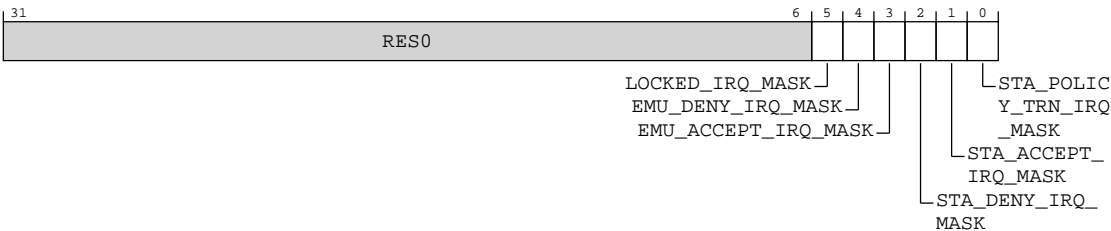


Table B-81: PPU\_IMR bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	LOCKED_IRQ_MASK	Locked event mask  0b0 Locked event enabled.  0b1 Locked event masked.	0b1

Bits	Name	Description	Reset
[4]	EMU_DENY_IRQ_MASK	Emulation transition denial event mask  <b>0b0</b> Emulation transition denial event enabled.  <b>0b1</b> Emulation transition denial event masked.	0b1
[3]	EMU_ACCEPT_IRQ_MASK	Emulation transition acceptance event mask  <b>0b0</b> Emulation transition acceptance event enabled.  <b>0b1</b> Emulation transition acceptance event masked.	0b1
[2]	STA_DENY_IRQ_MASK	Static transition denial event mask  <b>0b0</b> Static transition denial event enabled.  <b>0b1</b> Static transition denial event masked.	0b0
[1]	STA_ACCEPT_IRQ_MASK	Static transition acceptance event mask  <b>0b0</b> Static transition acceptance event enabled.  <b>0b1</b> Static transition acceptance event masked.	0b1
[0]	STA_POLICY_TRN_IRQ_MASK	Static full policy transition completion event mask  <b>0b0</b> Static full policy transition completion event enabled.  <b>0b1</b> Static full policy transition completion event masked.	0b0

## Accessibility

Component	Offset	Range
PPU	0x030	None

This interface is accessible as follows:

RW

### B.1.2.2.11 PPU\_AIMR, Additional Interrupt Mask Register

This register controls the events that assert the interrupt output. Additional event masking controls are in the Interrupt Mask Register (ext-PPU\_IMR), Input Edge Sensitivity Register (ext-PPU\_IESR), and the Operating Mode Active Edge Sensitivity Register (ext-PPU\_OPSR).

When an interrupt event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

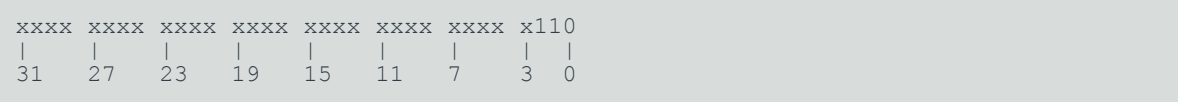
Register offset

0x034

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-42: EXT\_PPU\_AIMR bit assignments

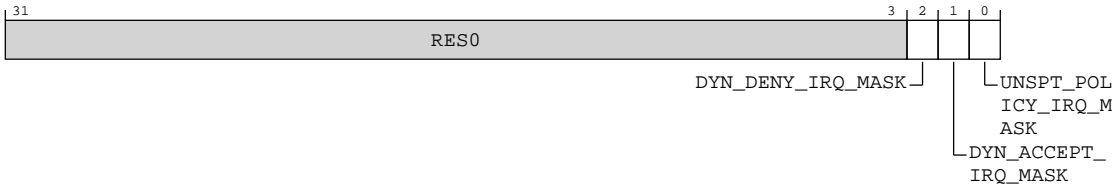


Table B-83: PPU\_AIMR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	DYN_DENY_IRQ_MASK	Dynamic transition denial event mask  0b0 Dynamic transition denial event enabled.  0b1 Dynamic transition denial event masked.	0b1

Bits	Name	Description	Reset
[1]	DYN_ACCEPT_IRQ_MASK	Dynamic transition acceptance event mask  <b>0b0</b> Dynamic transition acceptance event enabled.  <b>0b1</b> Dynamic transition acceptance event masked.	0b1
[0]	UNSPT_POLICY_IRQ_MASK	Unsupported policy event mask  <b>0b0</b> Unsupported policy event enabled.  <b>0b1</b> Unsupported policy event masked.	0b0

## Accessibility

Component	Offset	Range
PPU	0x034	None

This interface is accessible as follows:

RW

### B.1.2.2.12 PPU\_ISR, Interrupt Status Register

This register contains information about events causing the assertion of the interrupt output. It is also used to clear interrupt events.

A bit set to 0b1 indicates the event asserted the interrupt output. Multiple events can be active at the same time. When an interrupt event is masked an occurrence of that event does not set the status bit.

A write of 0b1 to an event bit clears that event. A write of 0b0 to a bit has no effect. The interrupt output stays HIGH until all status bits in the Interrupt Status Register (PPU\_ISR) and the Additional Interrupt Status Register (ext-PPU\_AISR) are 0b0.

When the OTHER\_IRQ bit is set, this indicates an event from the Additional Interrupt Status Register (PPU\_AISR) has caused the interrupt output to be asserted. This bit cannot be cleared by writing to this register. It must be cleared by writing to the active event in the Additional Interrupt Status Register (ext-PPU\_AISR).

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

Component

PPU

Register offset

0x038

Access type

RW1C

Reset value

xxxx	xxxx	xxxx	x000	0x0x	xx0x	0x00	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-43: EXT\_PPU\_ISR bit assignments

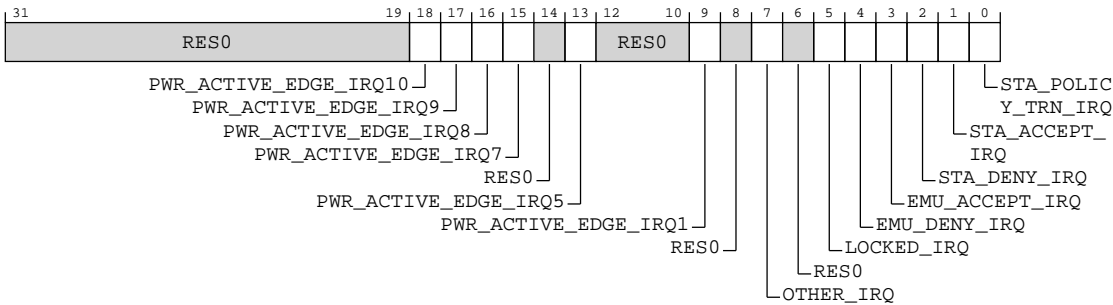


Table B-85: PPU\_ISR bit descriptions

Bits	Name	Description	Reset
[31:19]	RES0	Reserved	RES0
[18]	PWR_ACTIVE_EDGE_IRQ10	Indicates if power mode DEVPACTIVE[10] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[10] input (DBG_RECOV) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[10] input (DBG_RECOV) asserted the interrupt output.	0b0
[17]	PWR_ACTIVE_EDGE_IRQ9	Indicates if power mode DEVPACTIVE[9] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[9] input (WARM_RST) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[9] input (WARM_RST) asserted the interrupt output.	0b0

Bits	Name	Description	Reset
[16]	PWR_ACTIVE_EDGE_IRQ8	Indicates if power mode DEVPACTIVE[8] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[8] input (ON) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[8] input (ON) asserted the interrupt output.	0b0
[15]	PWR_ACTIVE_EDGE_IRQ7	Indicates if power mode DEVPACTIVE[7] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[7] input (FUNC_RET) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[7] input (FUNC_RET) asserted the interrupt output.	0b0
[14]	RES0	Reserved	RES0
[13]	PWR_ACTIVE_EDGE_IRQ5	Indicates if power mode DEVPACTIVE[5] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[5] input (FULL_RET) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[5] input (FULL_RET) asserted the interrupt output.	0b0
[12:10]	RES0	Reserved	RES0
[9]	PWR_ACTIVE_EDGE_IRQ1	Indicates if power mode DEVPACTIVE[1] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[1] input (OFF_EMU) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[1] input (OFF_EMU) asserted the interrupt output.	0b0
[8]	RES0	Reserved	RES0
[7]	OTHER_IRQ	Indicates there is an interrupt event pending in the Additional Interrupt Status Register (ext-PPU_AISR).  <b>0b0</b> No interrupt pending in ext-PPU_AISR.  <b>0b1</b> Interrupt pending in ext-PPU_AISR.	0b0
[6]	RES0	Reserved	RES0
[5]	LOCKED_IRQ	Locked event status.  <b>0b0</b> No locked event.  <b>0b1</b> A locked event asserted the interrupt output.	0b0
[4]	EMU_DENY_IRQ	Emulated transition denial event status.  <b>0b0</b> No emulated transition denial event.  <b>0b1</b> An emulated transition denial event asserted the interrupt output.	0b0

Bits	Name	Description	Reset
[3]	EMU_ACCEPT_IRQ	Emulated transition acceptance event status.  <b>0b0</b> No emulated transition acceptance event.  <b>0b1</b> An emulated transition acceptance event asserted the interrupt output.	0b0
[2]	STA_DENY_IRQ	Static transition denial event status.  <b>0b0</b> No static transition denial event.  <b>0b1</b> An static transition denial event asserted the interrupt output.	0b0
[1]	STA_ACCEPT_IRQ	Static transition acceptance event status.  <b>0b0</b> No static transition acceptance event.  <b>0b1</b> An static transition acceptance event asserted the interrupt output.	0b0
[0]	STA_POLICY_TRN_IRQ	Static full policy transition completion event status.  <b>0b0</b> No static full policy transition completion event.  <b>0b1</b> An static full policy transition completion event asserted the interrupt output.	0b0

## Accessibility

Component	Offset	Range
PPU	0x038	None

This interface is accessible as follows:

RW

### B.1.2.2.13 PPU\_AISR, Additional Interrupt Status Register

This register contains information about events causing the assertion of the interrupt output. It is also used to clear interrupt events.

A bit set to 0b1 indicates the event asserted the interrupt output. Multiple events can be active at the same time. When an interrupt event is masked an occurrence of that event does not set the status bit.

A write of 0b1 to an event bit clears that event. A write of 0b0 has no effect. The interrupt output stays HIGH until all status bits in the Interrupt Status Register (ext-PPU\_ISR) and the Additional Interrupt Status Register (PPU\_AISR) are set to 0b0.

When an interrupt status is set to 0b1 in this register it sets the OTHER\_IRQ bit in the Interrupt Status Register (ext-PPU\_ISR). Status bits in this register are only cleared by writing to this register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x03C

Access type

RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-44: EXT\_PPU\_AISR bit assignments

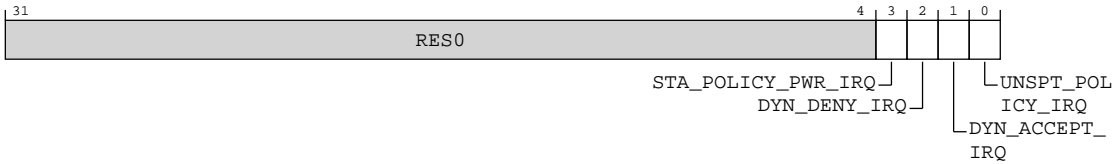


Table B-87: PPU\_AISR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3]	STA_POLICY_PWR_IRQ	Static power policy transition completion event status  <b>0b0</b> No static power policy transition completion event.  <b>0b1</b> A static power policy transition completion event asserted the interrupt output.	0b0



Bits	Name	Description	Reset
[2]	DYN_DENY_IRQ	Dynamic transition denial event status  <b>0b0</b> No dynamic transition denial event.  <b>0b1</b> A dynamic transition denial event asserted the interrupt output.	0b0
[1]	DYN_ACCEPT_IRQ	Dynamic transition acceptance event status  <b>0b0</b> No dynamic transition acceptance event.  <b>0b1</b> A dynamic transition acceptance event asserted the interrupt output.	0b0
[0]	UNSPT_POLICY_IRQ	Unsupported policy event status  <b>0b0</b> No unsupported policy event.  <b>0b1</b> An unsupported policy event asserted the interrupt output.	0b0

## Accessibility

Component	Offset	Range
PPU	0x03C	None

This interface is accessible as follows:

RW

### B.1.2.2.14 PPU\_IESR, Input Edge Sensitivity Register

This register configures the transitions on the power mode DEVPACTIVE inputs that generate an Input Edge interrupt event.

When an event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

PPU

### Register offset

0x040

Access type  
RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-45: EXT\_PPU\_IESR bit assignments

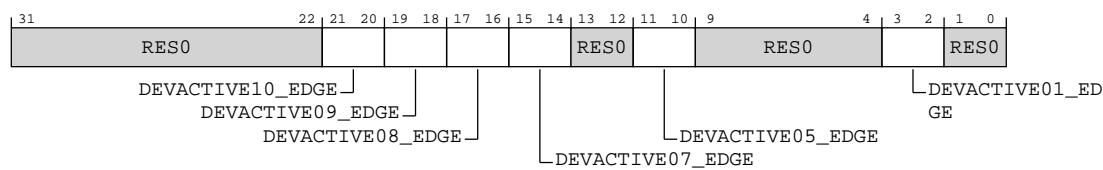


Table B-89: PPU\_IESR bit descriptions

Bits	Name	Description	Reset
[31:22]	RES0	Reserved	RES0
[21:20]	DEVACTIVE10_EDGE	Configures the transitions on the DEVPACTIVE[10] input (DBG_RECOV) that generate an Input Edge interrupt event.  <b>0b00</b> Event maksed.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00

Bits	Name	Description	Reset
[19:18]	DEVACTIVE09_EDGE	Configures the transitions on the DEVPACTIVE[9] input (WARM_RST) that generate an Input Edge interrupt event.  <b>0b00</b> Event masked.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[17:16]	DEVACTIVE08_EDGE	Configures the transitions on the DEVPACTIVE[8] input (ON) that generate an Input Edge interrupt event.  <b>0b00</b> Event masked.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[15:14]	DEVACTIVE07_EDGE	Configures the transitions on the DEVPACTIVE[7] input (FUNC_RET) that generate an Input Edge interrupt event.  <b>0b00</b> Event masked.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[13:12]	RES0	Reserved	RES0
[11:10]	DEVACTIVE05_EDGE	Configures the transitions on the DEVPACTIVE[5] input (FULL_RET) that generate an Input Edge interrupt event.  <b>0b00</b> Event masked.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[9:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3:2]	DEVACTIVE01_EDGE	Configures the transitions on the DEVPACTIVE[1] input (OFF_EMU) that generate an Input Edge interrupt event.  <b>0b00</b> Event maksed.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[1:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x040	None

This interface is accessible as follows:

RW

B.1.2.2.15 PPU\_OPSR, Operating Mode Active Edge Sensitivity Register

This register configures the transitions on the operating mode DEVPACTIVE inputs that generate an Input Edge interrupt event.

When an event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x044

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
------	------	------	------	------	------	------	------



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-46: EXT\_PPU\_OPSR bit assignments

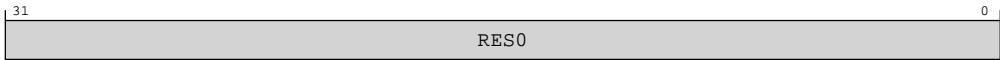


Table B-91: PPU\_OPSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x044	None

This interface is accessible as follows:

RW

B.1.2.2.16 PPU\_FUNRR, Functional Retention RAM Configuration Register

This register is reserved.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

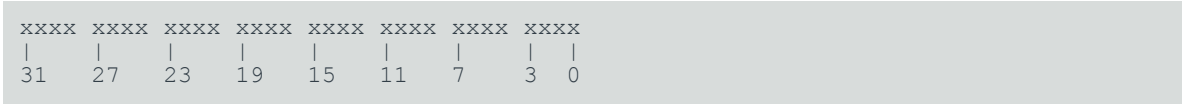
Register offset

0x050

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-47: EXT\_PPU\_FUNRR bit assignments

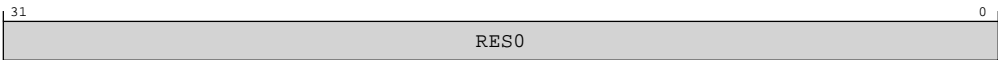


Table B-93: PPU\_FUNRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x050	None

This interface is accessible as follows:

RW

B.1.2.2.17 PPU\_FULRR, Full Retention RAM Configuration Register

This register is reserved (high bits of PCSMPSTATE outputs are not configurable by software).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x054

Access type  
RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-48: EXT\_PPU\_FULRR bit assignments



Table B-95: PPU\_FULRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x054	None

This interface is accessible as follows:

RW

B.1.2.2.18 PPU\_MEMRR, Memory Retention RAM Configuration Register

This register is reserved (high bits of PCSMPSTATE outputs are not configurable by software).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x058

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-49: EXT\_PPU\_MEMRR bit assignments

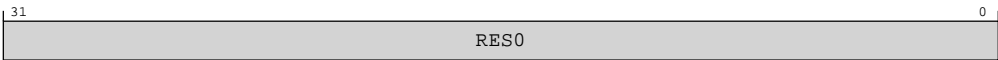


Table B-97: PPU\_MEMRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x058	None

This interface is accessible as follows:

RW

B.1.2.2.19 PPU\_EDTRO, Power Mode Entry Delay Register 0

This register is reserved (power mode entry delays not supported).

Configurations

This register is available in all configurations.

Attributes

Width

32



Component

PPU

Register offset

0x160

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-50: EXT\_PPU\_EDTR0 bit assignments

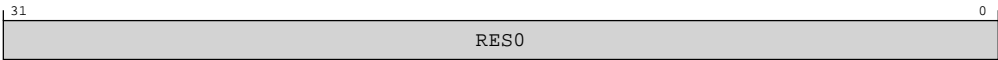


Table B-99: PPU\_EDTR0 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x160	None

This interface is accessible as follows:

RW

B.1.2.2.20 PPU\_EDTR1, Power Mode Entry Delay Register 1

This register is reserved (power mode entry delays not supported).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x164

Access type

RW

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-51: EXT\_PPU\_EDTR1 bit assignments

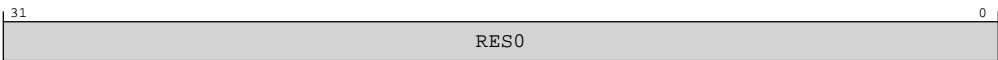


Table B-101: PPU\_EDTR1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0x164	None

This interface is accessible as follows:

RW

B.1.2.2.21 PPU\_DCDR0, Device Control Delay Configuration Register 0

This register is used to program device control delay parameters.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x170

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-52: EXT\_PPU\_DCDR0 bit assignments

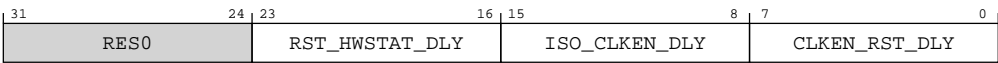


Table B-103: PPU\_DCDR0 bit descriptions

Bits	Name	Description	Reset
[31:24]	RES0	Reserved	RES0
[23:16]	RST_HWSTAT_DLY	Delay from reset de-assertion to HWSTAT update.	0x00
[15:8]	ISO_CLKEN_DLY	Delay from isolation enable de-assertion to clock enable assertion.	0x00
[7:0]	CLKEN_RST_DLY	Delay from clock enable assertion to reset de-assertion.	0x00

Accessibility

Component	Offset	Range
PPU	0x170	None

This interface is accessible as follows:

RW

B.1.2.2.22 PPU\_DCDR1, Device Control Delay Configuration Register 1

This register is used to program device control delay parameters.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0x174

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	0000	0000	0000	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-53: EXT\_PPU\_DCDR1 bit assignments

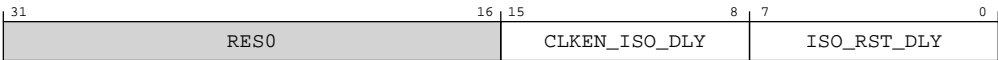


Table B-105: PPU\_DCDR1 bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0
[15:8]	CLKEN_ISO_DLY	Delay from clock enable de-assertion to isolation enable assertion.	0x00
[7:0]	ISO_RST_DLY	Delay from isolation enable assertion to reset assertion.	0x00

Accessibility

Component	Offset	Range
PPU	0x174	None

This interface is accessible as follows:

RW

B.1.2.2.23 PPU\_IDR0, PPU Identification Register 0

This read-only register contains information on the type and number of channels on the device interface and power and operating modes supported.

Additional information on optional features can be found in the PPU Identification Register 1 (ext-PPU\_IDR1).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFB0

Access type

RO

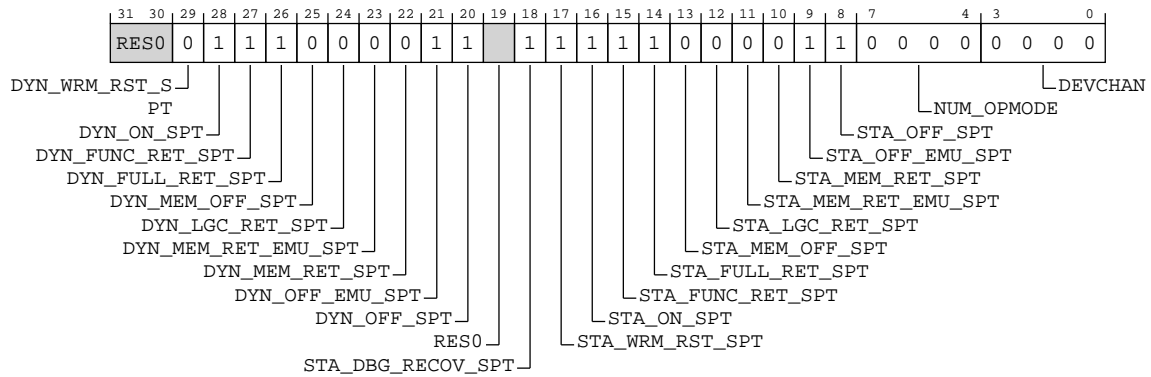
Reset value

xx01	1100	0011	x111	1100	0011	0000	0000
31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-54: EXT\_PPU\_IDR0 bit assignments****Table B-107: PPU\_IDR0 bit descriptions**

Bits	Name	Description	Reset
[31:30]	RES0	Reserved	RES0
[29]	DYN_WRM_RST_SPT	Dynamic WARM_RST support. <b>0b0</b> Dynamic WARM_RST not supported.	0b0
[28]	DYN_ON_SPT	Dynamic ON support. <b>0b1</b> Dynamic ON supported.	0b1
[27]	DYN_FUNC_RET_SPT	Dynamic DYN_FUNC_RET_SPT support. <b>0b1</b> Dynamic DYN_FUNC_RET_SPT supported.	0b1
[26]	DYN_FULL_RET_SPT	Dynamic DYN_FULL_RET_SPT support. <b>0b1</b> Dynamic DYN_FULL_RET_SPT supported.	0b1
[25]	DYN_MEM_OFF_SPT	Dynamic MEM_OFF support. <b>0b0</b> Dynamic MEM_OFF not supported.	0b0
[24]	DYN_LGC_RET_SPT	Dynamic LOGIC_RET support. <b>0b0</b> Dynamic LOGIC_RET not supported.	0b0

Bits	Name	Description	Reset
[23]	DYN_MEM_RET_EMU_SPT	Dynamic DYN_MEM_RET_EMU_SPT support. <b>0b0</b> Dynamic DYN_MEM_RET_EMU_SPT not supported.	0b0
[22]	DYN_MEM_RET_SPT	Dynamic DYN_MEM_RET_SPT support. <b>0b0</b> Dynamic DYN_MEM_RET_SPT not supported.	0b0
[21]	DYN_OFF_EMU_SPT	Dynamic OFF_EMU support. <b>0b1</b> Dynamic OFF_EMU supported.	0b1
[20]	DYN_OFF_SPT	Dynamic OFF support. <b>0b1</b> Dynamic OFF supported.	0b1
[19]	<b>RES0</b>	Reserved	<b>RES0</b>
[18]	STA_DBG_RECOV_SPT	DBG_RECOV support. <b>0b1</b> DBG_RECOV supported.	0b1
[17]	STA_WRM_RST_SPT	WRM_RST support. <b>0b1</b> WRM_RST supported.	0b1
[16]	STA_ON_SPT	ON support. <b>0b1</b> ON supported.	0b1
[15]	STA_FUNC_RET_SPT	FUNC_RET support. <b>0b1</b> FUNC_RET supported.	0b1
[14]	STA_FULL_RET_SPT	FULL_RET support. <b>0b1</b> FULL_RET supported.	0b1
[13]	STA_MEM_OFF_SPT	MEM_OFF support. <b>0b0</b> MEM_OFF not supported.	0b0
[12]	STA_LGC_RET_SPT	LOGIC_RET support. <b>0b0</b> LOGIC_RET not supported.	0b0
[11]	STA_MEM_RET_EMU_SPT	MEM_RET_EMU support. <b>0b0</b> MEM_RET_EMU not supported.	0b0
[10]	STA_MEM_RET_SPT	MEM_RET support. <b>0b0</b> MEM_RET not supported.	0b0

Bits	Name	Description	Reset
[9]	STA_OFF_EMU_SPT	OFF_EMU support. <b>0b1</b> OFF_EMU supported.	0b1
[8]	STA_OFF_SPT	OFF support. <b>0b1</b> OFF supported.	0b1
[7:4]	NUM_OPMODE	No. of operating modes supported, minus 1. <b>0b0000</b> 1 operating mode supported.	0b0000
[3:0]	DEVCHAN	No. of Device Interface Channels. <b>0b0000</b> 0 (P-channel PPU).	0b0000

### Accessibility

Component	Offset	Range
PPU	0xFB0	None

This interface is accessible as follows:

RO

#### B.1.2.2.24 PPU\_IDR1, PPU Identification Register 1

This read-only register contains information on the optional features and configurations that are supported by this PPU.

Additional information on optional features can be found in the PPU Identification Register 0 (ext-PPU\_IDR0).

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

PPU

#### Register offset

0xFB4

#### Access type

RO



## Reset value

xxxx	xxxx	xxxx	xxxx	xxx0	xxx0	x000	x110
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-55: EXT\_PPU\_IDR1 bit assignments

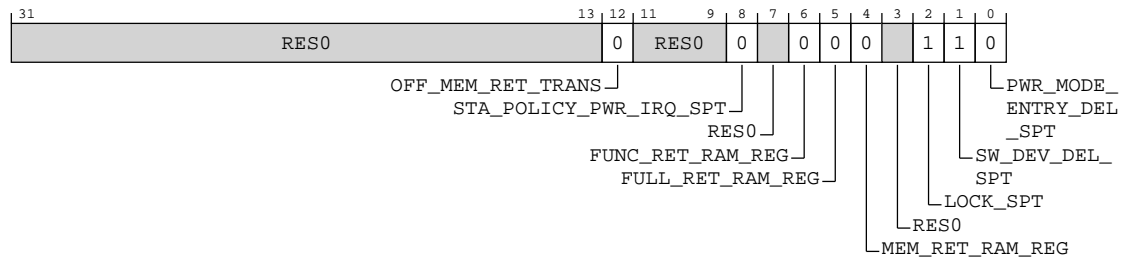


Table B-109: PPU\_IDR1 bit descriptions

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0
[12]	OFF_MEM_RET_TRANS	OFF to MEM_RET direct transition. Indicates if direct transitions from OFF to MEM_RET and from OFF_EMU to MEM_RET_EMU are supported.  <b>0b0</b> OFF to MEM_RET direct transition not supported.	0b0
[11:9]	RES0	Reserved	RES0
[8]	STA_POLICY_PWR_IRQ_SPT	Power policy transition completion event status.  <b>0b0</b> Power policy transition completion events not supported.	0b0
[7]	RES0	Reserved	RES0
[6]	FUNC_RET_RAM_REG	Indicates if the ext-PPU_FUNRR register is present or reserved.  <b>0b0</b> ext-PPU_FUNRR is reserved.	0b0
[5]	FULL_RET_RAM_REG	Indicates if the ext-PPU_FULRR register is present or reserved.  <b>0b0</b> ext-PPU_FULRR is not present.	0b0
[4]	MEM_RET_RAM_REG	Indicates if the ext-PPU_MEMRR register is present or reserved.  <b>0b0</b> ext-PPU_MEMRR is reserved.	0b0
[3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2]	LOCK_SPT	Indicates if the lock and the lock interrupt event are supported.  <b>0b1</b> Lock and the lock interrupt event are supported.	0b1
[1]	SW_DEV_DEL_SPT	Software device delay control configuration support.  <b>0b1</b> Software device delay control configuration supported.	0b1
[0]	PWR_MODE_ENTRY_DEL_SPT	Power mode entry delay support.  <b>0b0</b> Power mode entry delay not supported.	0b0

## Accessibility

Component	Offset	Range
PPU	0xFB4	None

This interface is accessible as follows:

RO

### B.1.2.2.25 PPU\_IIDR, Implementation Identification Register

This register provides information about the implementer and implementation of the PPU.

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

PPU

### Register offset

0xFC8

### Access type

RO

### Reset value

0000 1011 0110 0001 0001 0100 0011 1011

Bit descriptions

Figure B-56: EXT\_PPU\_IIDR bit assignments

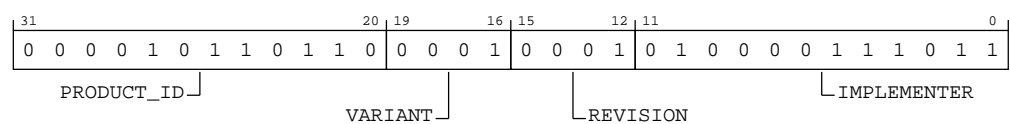


Table B-111: PPU\_IIDR bit descriptions

Bits	Name	Description	Reset
[31:20]	PRODUCT_ID	Value identifying the PPU part.  <b>0b0000010110110</b> PCK-600 PPU.	0x0B6
[19:16]	VARIANT	Value used to distinguish product variants, or major revisions of the product.  <b>0b0001</b> Product variant r0p5.	0b0001
[15:12]	REVISION	Value used to distinguish minor revisions of the product.  <b>0b0001</b> No ECO fixes.	0b0001
[11:0]	IMPLEMENTER	Implementer identification.  <b>0b010000111011</b> Arm Limited.	0x43B

Accessibility

Component	Offset	Range
PPU	0xFC8	None

This interface is accessible as follows:

RO

B.1.2.2.26 PPU\_AIDR, Architecture Identification Register

This register identifies the PPU architecture revision.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFCC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0001
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-57: EXT\_PPU\_AIDR bit assignments

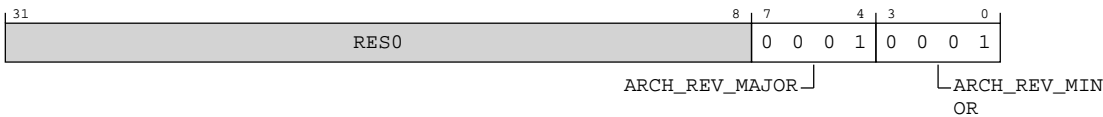


Table B-113: PPU\_AIDR bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	ARCH_REV_MAJOR	PPU architecture major revision.  0b0001 PPU architecture major revision 1.	0b0001
[3:0]	ARCH_REV_MINOR	PPU architecture minor revision.  0b0001 PPU architecture minor revision 1.	0b0001

Accessibility

Component	Offset	Range
PPU	0xFCC	None

This interface is accessible as follows:

RO

B.1.2.2.27 PPU\_PIDR4, PPU Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFD0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-58: EXT\_PPU\_PIDR4 bit assignments

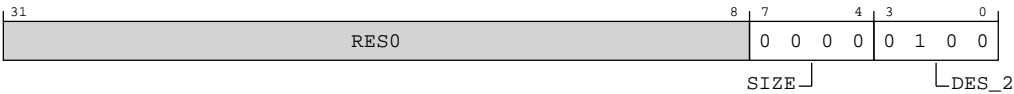


Table B-115: PPU\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count.  0b0000 The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code.  0b0100 Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
PPU	0xFD0	None

This interface is accessible as follows:

RO

B.1.2.2.28 PPU\_PIDR5, PPU Peripheral Identification Register 5

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFD4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-59: EXT\_PPU\_PIDR5 bit assignments



Table B-117: PPU\_PIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0xFD4	None

This interface is accessible as follows:

RO

B.1.2.2.29 PPU\_PIDR6, PPU Peripheral Identification Register 6

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFD8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-60: EXT\_PPU\_PIDR6 bit assignments

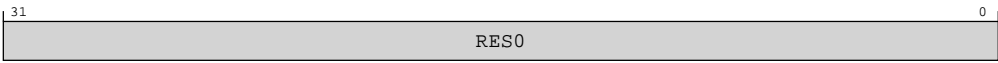


Table B-119: PPU\_PIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0xFD8	None

This interface is accessible as follows:

RO

B.1.2.2.30 PPU\_PIDR7, PPU Peripheral Identification Register 7

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

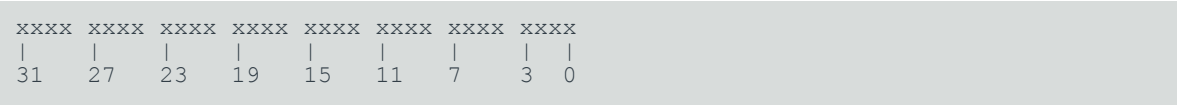
Register offset

0xFDC

Access type

RO

Reset value







Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-61: EXT\_PPU\_PIDR7 bit assignments

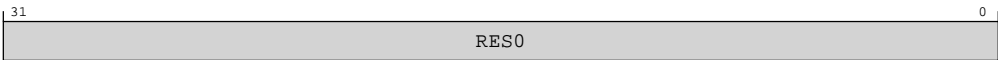


Table B-121: PPU\_PIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
PPU	0xFDC	None

This interface is accessible as follows:

RO

B.1.2.2.31 PPU\_PIDR0, PPU Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFE0

Access type

RO

Reset value

xxxx xxxx xxxx xxxx xxxx xxxx 1011 0110



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-62: EXT\_PPU\_PIDR0 bit assignments



Table B-123: PPU\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b10110110 PCK-600 PPU. Bits [7:0] of part number 0x0B6.	0xB6

Accessibility

Component	Offset	Range
PPU	0xFE0	None

This interface is accessible as follows:

RO

B.1.2.2.32 PPU\_PIDR1, PPU Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFE4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-63: EXT\_PPU\_PIDR1 bit assignments



Table B-125: PPU\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0].  <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8].  <b>0b0000</b> PCK-600 PPU. Bits [11:8] of part number 0x0B6.	0b0000

Accessibility

Component	Offset	Range
PPU	0xFE4	None

This interface is accessible as follows:

RO

B.1.2.2.33 PPU\_PIDR2, PPU Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

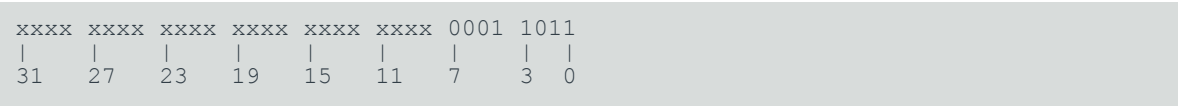
Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-64: EXT\_PPU\_PIDR2 bit assignments

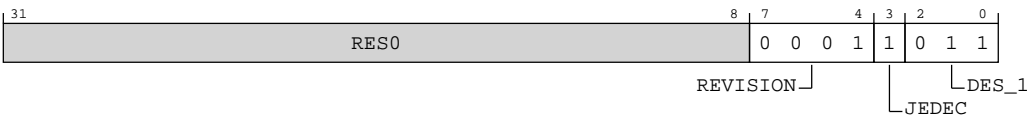


Table B-127: PPU\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0001 Revision r0p5.	0b0001

Bits	Name	Description	Reset
[3]	JEDEC	JEDEC assignee.  <b>0b1</b> JEDEC-assignee values is used.	0b1
[2:0]	DES_1	JEP106 identification code bits [6:4].  <b>0b011</b> Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
PPU	0xFE8	None

This interface is accessible as follows:

RO

B.1.2.2.34 PPU\_PIDR3, PPU Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFE8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-65: EXT\_PPU\_PIDR3 bit assignments

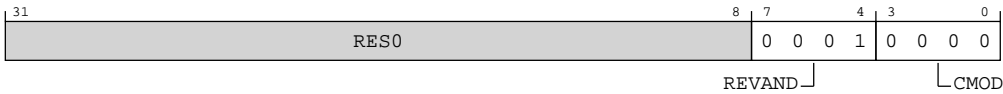


Table B-129: PPU\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes. <b>0b0001</b> No ECO fixes.	0b0001
[3:0]	CMOD	Customer Modified. <b>0b0000</b> The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
PPU	0xFEC	None

This interface is accessible as follows:

RO

B.1.2.2.35 PPU\_CIDR0, PPU Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

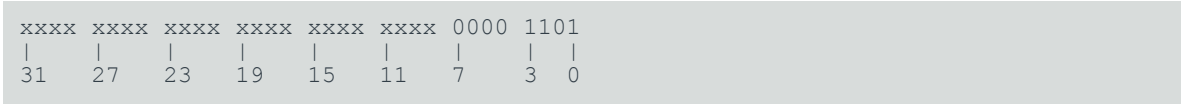
Register offset

0xFF0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-66: EXT\_PPU\_CIDR0 bit assignments



Table B-131: PPU\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble.  0b00001101 CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
PPU	0xFF0	None

This interface is accessible as follows:

RO

B.1.2.2.36 PPU\_CIDR1, PPU Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

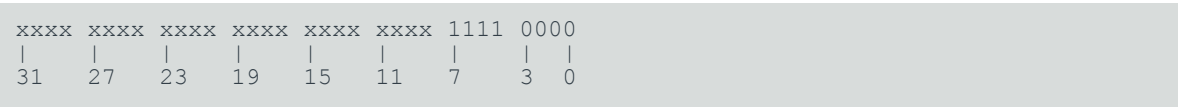
Register offset

0xFF4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-67: EXT\_PPU\_CIDR1 bit assignments



Table B-133: PPU\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1111</b> CoreLink component.	0b1111
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
PPU	0xFF4	None

This interface is accessible as follows:

RO



B.1.2.2.37 PPU\_CIDR2, PPU Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

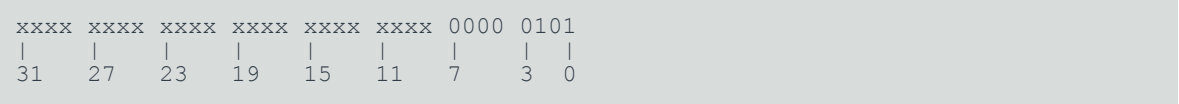
Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-68: EXT\_PPU\_CIDR2 bit assignments

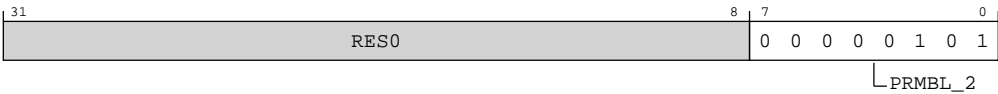


Table B-135: PPU\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble.  0b000000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
PPU	0xFF8	None

This interface is accessible as follows:

RO

B.1.2.2.38 PPU\_CIDR3, PPU Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PPU

Register offset

0xFFC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0001
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-69: EXT\_PPU\_CIDR3 bit assignments

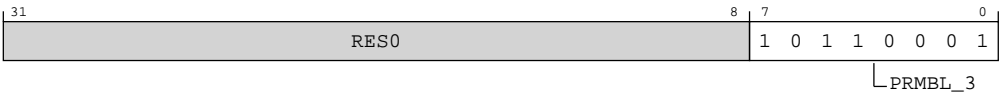


Table B-137: PPU\_CIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble.  <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
PPU	0xFFC	None

This interface is accessible as follows:

RO

B.1.2.3 External CLUSTERPPU register description

This section includes the register descriptions for all memory-mapped CLUSTERPPU registers that are accessed for the cluster.

B.1.2.3.1 CLUSTERPPU\_PWPR, Power Policy Register

This register enables software to program both power and operating mode policy. It also contains related settings including the enable for dynamic transitions and the lock enable.

This register does not reflect the current power mode value. The current power mode of the domain is reflected in the Power Status Register (ext-CLUSTERPPU\_PWSR).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x000

Access type

RW

Reset value

xxxx xxx0 xxxx xxxx xxx0 xxx1 xxxx 0000



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-70: EXT\_CLUSTERPPU\_PWPR bit assignments

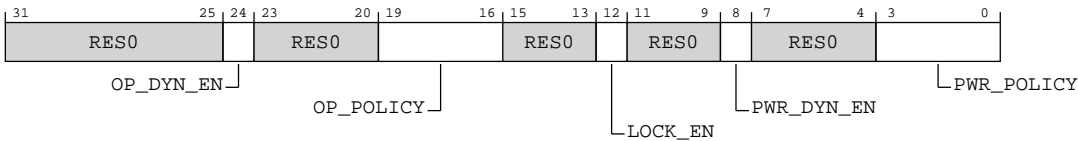


Table B-139: CLUSTERPPU\_PWPR bit descriptions

Bits	Name	Description	Reset
[31:25]	RES0	Reserved	RES0
[24]	OP_DYN_EN	Operating mode dynamic transition enable.  <b>0b0</b> Dynamic transitions disabled for operating modes.  <b>0b1</b> Dynamic transitions enabled for operating modes, allowing transitions to be initiated by changes on operating mode DEVACTIVE inputs.	0b0
[23:20]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[19:16]	OP_POLICY	<p><b>When L2_SLICES == 2</b></p> <p>Operating mode policy.</p> <p>When static operating mode transitions are enabled, OP_DYN_EN is set to 0b0, then this is the target operating mode for the PPU.</p> <p>When dynamic operating mode transitions are enabled, OP_DYN_EN is set to 0b1, then this is the minimum operating mode for the PPU.</p> <p><b>0b0000</b></p> <p>OPMODE_00: The L2 Cache is not operational.</p> <p><b>0b0001</b></p> <p>OPMODE_01: Half of the L2 Cache is operational.</p> <p><b>0b0010</b></p> <p>OPMODE_02: The whole L2 Cache is operational.</p> <p><b>Otherwise</b></p> <p>Operating mode policy.</p> <p>When static operating mode transitions are enabled, OP_DYN_EN is set to 0b0, then this is the target operating mode for the PPU.</p> <p>When dynamic operating mode transitions are enabled, OP_DYN_EN is set to 0b1, then this is the minimum operating mode for the PPU.</p> <p><b>0b0000</b></p> <p>OPMODE_00: The L2 Cache is not operational.</p> <p><b>0b0010</b></p> <p>OPMODE_02: The whole L2 Cache is operational.</p>	xxxx
[15:13]	RES0	Reserved	RES0
[12]	LOCK_EN	<p>Lock enable bit.</p> <p><b>0b0</b></p> <p>Lock feature disabled.</p> <p><b>0b1</b></p> <p>Lock feature enabled.</p>	0b0
[11:9]	RES0	Reserved	RES0
[8]	PWR_DYN_EN	<p>Power mode dynamic transition enable.</p> <p><b>0b0</b></p> <p>Dynamic transitions disabled for power modes.</p> <p><b>0b1</b></p> <p>Dynamic transitions enabled for power modes, allowing transitions to be initiated by changes on power mode DEACTIVE inputs.</p>	0b1
[7:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3:0]	PWR_POLICY	<p>Power mode policy.</p> <p>When static power mode transitions are enabled, PWR_DYN_EN is set to 0b0, this is the target power mode for the CLUSTERPPU.</p> <p>When dynamic power mode transitions are enabled, PWR_DYN_EN is set to 0b1, this is the minimum power mode for the CLUSTERPPU.</p> <p><b>0b0000</b> OFF. Logic off and RAM off.</p> <p><b>0b0001</b> OFF_EMU. Emulated Off. Logic on with RAM on. This mode is used to emulate the functional condition of OFF without removing power.</p> <p><b>0b0010</b> MEM_RET. Memory Retention. Logic off with RAM retained.</p> <p><b>0b0011</b> MEM_RET_EMU. Emulated Memory Retention. Logic on with RAM on. This mode is used to emulate the functional condition of MEM_RET without removing power.</p> <p><b>0b1000</b> ON. Logic on with RAM on, cluster is functional.</p> <p><b>0b1001</b> WARM_RST. Warm Reset. Warm reset application with logic and RAM on.</p> <p><b>0b1010</b> DBG_RECOV. Debug Recovery Reset. Warm reset application with logic and RAM on.</p>	0b0000

## Accessibility

Component	Offset	Range
CLUSTERPPU	0x000	None

This interface is accessible as follows:

RW

### B.1.2.3.2 CLUSTERPPU\_PMER, Power Mode Emulation Enable Register

This register allows software to enable entry into emulated modes.

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

CLUSTERPPU

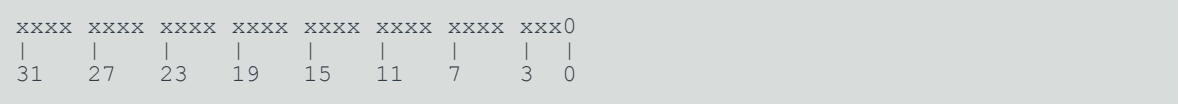
Register offset

0x004

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-71: EXT\_CLUSTERPPU\_PMER bit assignments

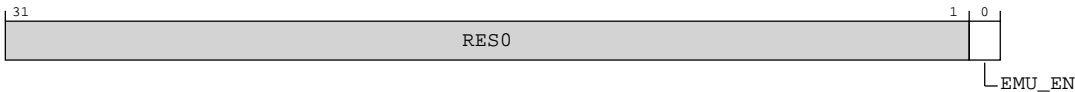


Table B-141: CLUSTERPPU\_PMER bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	EMU_EN	Power mode emulation enable.  0b0 Power mode emulation disabled.  0b1 Power mode emulation enabled. Transitions to OFF and MEM_RET instead transition to OFF_EMU and MEM_RET_EMU.	0b0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x004	None

This interface is accessible as follows:

RW

B.1.2.3.3 CLUSTERPPU\_PWSR, Power Status Register

This read-only register contains status information for the power mode, operating mode, dynamic transitions, and lock feature.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x008

Access type

RO

Reset value

xxxx	xxx0	xxxx	xxxx	xxx0	xxx1	xxxx	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-72: EXT\_CLUSTERPPU\_PWSR bit assignments

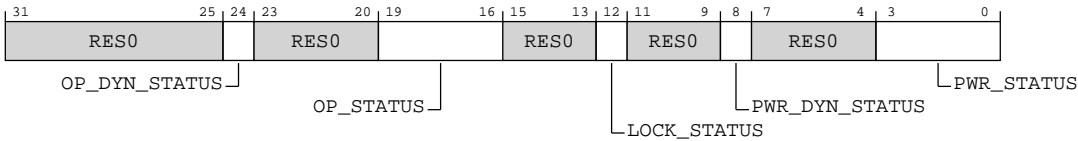


Table B-143: CLUSTERPPU\_PWSR bit descriptions

Bits	Name	Description	Reset
[31:25]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[24]	OP_DYN_STATUS	<p>Operating mode dynamic transition status.</p> <p>There might be a delay in dynamic transitions becoming active or inactive if the PPU is transitioning when ext-CLUSTERPPU_PWPR.OP_DYN_EN is programmed.</p> <p><b>0b0</b></p> <p>Dynamic transitions disabled for operating modes.</p> <p><b>0b1</b></p> <p>Dynamic transitions enabled for operating modes.</p>	0b0
[23:20]	RES0	Reserved	RES0
[19:16]	OP_STATUS	<p><b>When L2_SLICES == 2</b></p> <p>Operating mode status.</p> <p>These bits reflect the current operating mode of the PPU.</p> <p>In the OFF, OFF_EMU, DBG_RECOV, and WARM_RST power modes, this field reflects the current programmed OP_POLICY even though the operating mode DEVPSTATE output bits are set to zero.</p> <p><b>0b0000</b></p> <p>OPMODE_00: The L2 Cache is not operational.</p> <p><b>0b0001</b></p> <p>OPMODE_01: Half of the L2 Cache is operational.</p> <p><b>0b0010</b></p> <p>OPMODE_02: The whole L2 Cache is operational.</p> <p><b>Otherwise</b></p> <p>Operating mode status.</p> <p>These bits reflect the current operating mode of the PPU.</p> <p>In the OFF, OFF_EMU, DBG_RECOV, and WARM_RST power modes, this field reflects the current programmed OP_POLICY even though the operating mode DEVPSTATE output bits are set to zero.</p> <p><b>0b0000</b></p> <p>OPMODE_00: The L2 Cache is not operational.</p> <p><b>0b0010</b></p> <p>OPMODE_02: The whole L2 Cache is operational.</p>	xxxx
[15:13]	RES0	Reserved	RES0
[12]	LOCK_STATUS	<p>Lock status.</p> <p><b>0b0</b></p> <p>The PPU is not locked in the current mode.</p> <p><b>0b1</b></p> <p>The PPU is locked in the current mode.</p>	0b0
[11:9]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[8]	PWR_DYN_STATUS	Power mode dynamic transition status.  There might be a delay in dynamic transitions becoming active or inactive if the PPU is transitioning when ext-CLUSTERPPU_PWPR.DYN_EN is programmed.  <b>0b0</b> Dynamic transitions disabled for power modes.  <b>0b1</b> Dynamic transitions enabled for power modes.	0b1
[7:4]	RES0	Reserved	RES0
[3:0]	PWR_STATUS	Power mode status.  These bits reflect the current power mode of the PPU.  <b>0b0000</b> OFF. Logic off and RAM off.  <b>0b0001</b> OFF_EMU. Emulated Off. Logic on with RAM on. This mode is used to emulate the functional condition of OFF without removing power.  <b>0b0010</b> MEM_RET. Memory Retention. Logic off with RAM retained.  <b>0b0011</b> MEM_RET_EMU. Emulated Memory Retention. Logic on with RAM on. This mode is used to emulate the functional condition of MEM_RET without removing power.  <b>0b1000</b> ON. Logic on with RAM on, cluster is functional.  <b>0b1001</b> WARM_RST. Warm Reset. Warm reset application with logic and RAM on.  <b>0b1010</b> DBG_RECOV. Debug Recovery Reset. Warm reset application with logic and RAM on.	0b0000

## Accessibility

Component	Offset	Range
CLUSTERPPU	0x008	None

This interface is accessible as follows:

RO

### B.1.2.3.4 CLUSTERPPU\_DISR, Device Interface Input Current Status Register

This read-only register contains status reflecting the values of the device interface inputs.

## Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

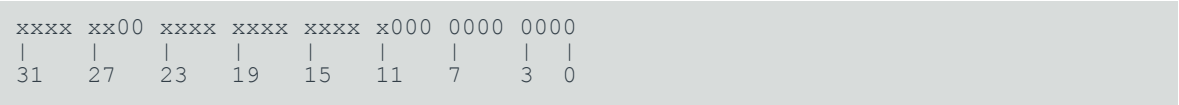
Register offset

0x010

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-73: EXT\_CLUSTERPPU\_DISR bit assignments

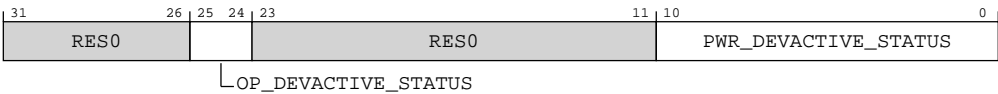


Table B-145: CLUSTERPPU\_DISR bit descriptions

Bits	Name	Description	Reset
[31:26]	RES0	Reserved	RES0
[25:24]	OP_DEVACTIVE_STATUS	Status of the operating mode DEVPACTIVE inputs.  <b>0b00</b> Request for OPMODE_00.  <b>0b01</b> Request for OPMODE_01.  <b>1x</b> Request for OPMODE_02.	0b00
[23:11]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[10:0]	PWR_DEVACTIVE_STATUS	<p>Status of the power mode DEVPACTIVE inputs.</p> <p><b>0b000000000000</b> Request for OFF.</p> <p><b>0000000001x</b> Request for OFF_EMU.</p> <p><b>000000001xx</b> Request for MEM_RET.</p> <p><b>00000001xxx</b> Request for MEM_RET_EMU.</p> <p><b>001xxxxxxxxx</b> Request for ON.</p> <p><b>01xxxxxxxxxx</b> Request for WARM_RST.</p> <p><b>1xxxxxxxxxxx</b> Request for DBG_RECOV.</p>	0b000000000000

### Accessibility

Component	Offset	Range
CLUSTERPPU	0x010	None

This interface is accessible as follows:

RO

#### B.1.2.3.5 CLUSTERPPU\_MISR, Miscellaneous Input Current Status Register

This read-only register contains status reflecting the values of miscellaneous inputs.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

CLUSTERPPU

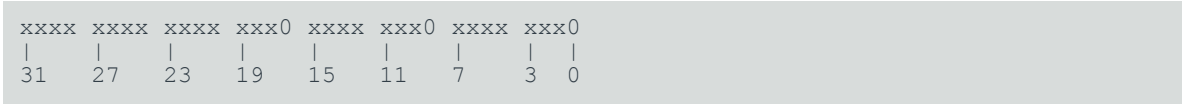
#### Register offset

0x014

#### Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-74: EXT\_CLUSTERPPU\_MISR bit assignments

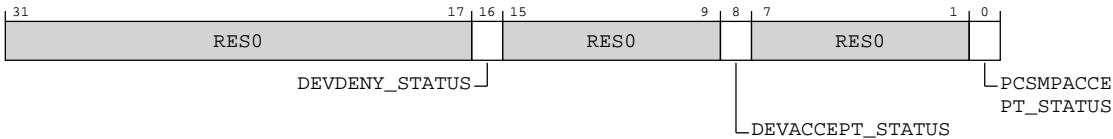


Table B-147: CLUSTERPPU\_MISR bit descriptions

Bits	Name	Description	Reset
[31:17]	RES0	Reserved	RES0
[16]	DEVDPENY_STATUS	Status of the device interface DEVPDENY inputs.  0b0 DEVPDENY deasserted.  0b1 DEVPDENY asserted.	0b0
[15:9]	RES0	Reserved	RES0
[8]	DEVACCEPT_STATUS	Status of the device interface DEVPACCEPT inputs.  0b0 DEVPACCEPT deasserted.  0b1 DEVPACCEPT asserted.	0b0
[7:1]	RES0	Reserved	RES0
[0]	PCSMACCEPT_STATUS	Status of the PCSMAPCEPT inputs.  0b0 PCSMACCEPT deasserted.  0b1 PCSMACCEPT asserted.	0b0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x014	None

This interface is accessible as follows:

RO

B.1.2.3.6 CLUSTERPPU\_STSR, Stored Status Register

This register is reserved for P-channel PPU.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x018

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-75: EXT\_CLUSTERPPU\_STSR bit assignments



Table B-149: CLUSTERPPU\_STSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x018	None

This interface is accessible as follows:

RO

B.1.2.3.7 CLUSTERPPU\_UNLK, Unlock Register

This register allows software to unlock the PPU from a locked power mode.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

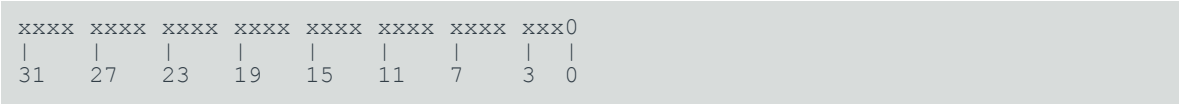
Register offset

0x01C

Access type

RAZW

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-76: EXT\_CLUSTERPPU\_UNLK bit assignments

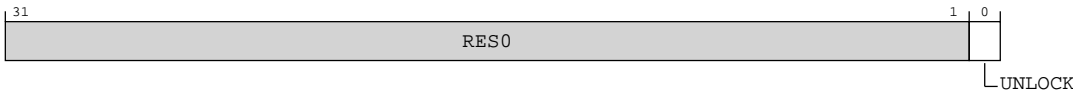


Table B-151: CLUSTERPPU\_UNLK bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	UNLOCK	When 0b1 is written to this bit the PPU is unlocked from a locked power mode. A read always returns 0b0.	0b0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x01C	None

This interface is accessible as follows:

RW

B.1.2.3.8 CLUSTERPPU\_PWCR, Power Configuration Register

This register controls enabling and disabling of hardware control inputs to the PPU.



Before software programs the DEVREQEN bits it must configure the PPU for static transitions and ensure the requested power mode has been reached, this means that no further transitions can occur, otherwise behavior is UNPREDICTABLE.

The PWR\_DEVACTIVEEN and OP\_DEVACTIVEEN fields in this register control the ability of the DEVACTIVE inputs to initiate power mode transitions, but not the ability to generate input edge interrupt events.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x020

Access type

RW

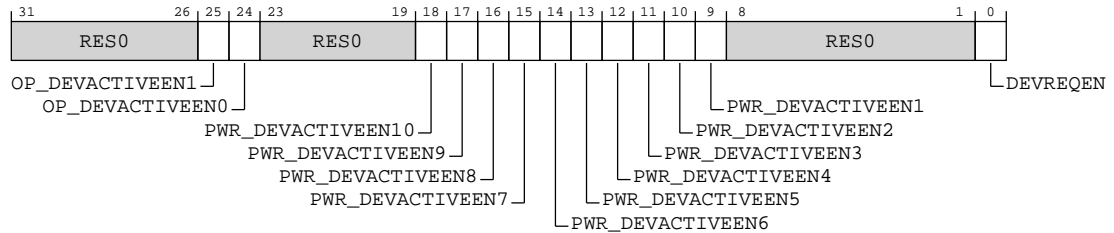
Reset value

xxxx	xx11	xxxx	x111	1111	111x	xxxx	xxx1
31	27	23	19	15	11	7	3 0



**Note**

Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure B-77: EXT\_CLUSTERPPU\_PWCR bit assignments****Table B-153: CLUSTERPPU\_PWCR bit descriptions**

Bits	Name	Description	Reset
[31:26]	<b>RES0</b>	Reserved	<b>RES0</b>
[25]	OP_DEVACTIVEEN1	Enables the operating mode DEVPACTIVE[17] input. <b>0b0</b> DEVPACTIVE[17] input (OPMODE_02) disabled. <b>0b1</b> DEVPACTIVE[17] input (OPMODE_02) enabled.	0b1
[24]	OP_DEVACTIVEEN0	Enables the operating mode DEVPACTIVE[16] input. <b>0b0</b> DEVPACTIVE[16] input (OPMODE_01) disabled. <b>0b1</b> DEVPACTIVE[16] input (OPMODE_01) enabled.	0b1
[23:19]	<b>RES0</b>	Reserved	<b>RES0</b>
[18]	PWR_DEVACTIVEEN10	Enables the operating mode DEVPACTIVE[10] input. <b>0b0</b> DEVPACTIVE[10] input (DBG_RECOV) disabled. <b>0b1</b> DEVPACTIVE[10] input (DBG_RECOV) enabled.	0b1
[17]	PWR_DEVACTIVEEN9	Enables the operating mode DEVPACTIVE[9] input. <b>0b0</b> DEVPACTIVE[9] input (WARM_RST) disabled. <b>0b1</b> DEVPACTIVE[9] input (WARM_RST) enabled.	0b1

Bits	Name	Description	Reset
[16]	PWR_DEVACTIVEEN8	Enables the operating mode DEVACTIVE[8] input. <b>0b0</b> DEVACTIVE[8] input (ON) disabled. <b>0b1</b> DEVACTIVE[8] input (ON) enabled.	0b1
[15]	PWR_DEVACTIVEEN7	Enables the operating mode DEVACTIVE[7] input. <b>0b0</b> DEVACTIVE[7] input (unused) disabled. <b>0b1</b> DEVACTIVE[7] input (unused) enabled.	0b1
[14]	PWR_DEVACTIVEEN6	Enables the operating mode DEVACTIVE[6] input. <b>0b0</b> DEVACTIVE[6] input (unused) disabled. <b>0b1</b> DEVACTIVE[6] input (unused) enabled.	0b1
[13]	PWR_DEVACTIVEEN5	Enables the operating mode DEVACTIVE[5] input. <b>0b0</b> DEVACTIVE[5] input (unused) disabled. <b>0b1</b> DEVACTIVE[5] input (unused) enabled.	0b1
[12]	PWR_DEVACTIVEEN4	Enables the operating mode DEVACTIVE[4] input. <b>0b0</b> DEVACTIVE[4] input (unused) disabled. <b>0b1</b> DEVACTIVE[4] input (unused) enabled.	0b1
[11]	PWR_DEVACTIVEEN3	Enables the operating mode DEVACTIVE[3] input. <b>0b0</b> DEVACTIVE[3] input (MEM_RET_EMU) disabled. <b>0b1</b> DEVACTIVE[3] input (MEM_RET_EMU) enabled.	0b1
[10]	PWR_DEVACTIVEEN2	Enables the operating mode DEVACTIVE[2] input. <b>0b0</b> DEVACTIVE[2] input (MEM_RET) disabled. <b>0b1</b> DEVACTIVE[2] input (MEM_RET) enabled.	0b1
[9]	PWR_DEVACTIVEEN1	Enables the operating mode DEVACTIVE[1] input. <b>0b0</b> DEVACTIVE[1] input (OFF_EMU) disabled. <b>0b1</b> DEVACTIVE[1] input (OFF_EMU) enabled.	0b1
[8:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	DEVREQEN	Device interface handshake enable.  <b>0b0</b> Device interface handshake disabled for transitions.  <b>0b1</b> Device interface handshake enabled for transitions.	0b1

Accessibility

Component	Offset	Range
CLUSTERPPU	0x020	None

This interface is accessible as follows:

RW

B.1.2.3.9 CLUSTERPPU\_PTCR, Power Mode Transition Register

This register contains settings which affect the behaviour of certain power mode transitions.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x024

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx01
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-78: EXT\_CLUSTERPPU\_PTCR bit assignments

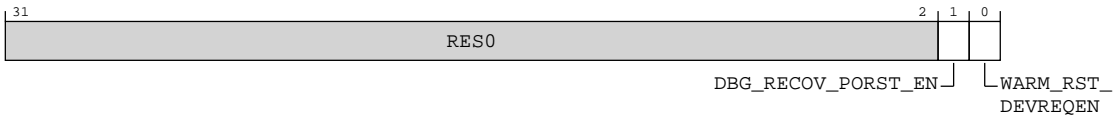


Table B-155: CLUSTERPPU\_PTCR bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	DBG_RECOV_PORST_EN	<p>Power-on reset behavior in DBG_RECOV.</p> <p>This bit should not be modified when the PPU is in DBG_RECOV. If it is modified, it will not have any effect on the reset output.</p> <p>This bit should not be modified when the PPU is in transition. If it is modified, the reset output will depend on either the old or the new value of the bit.</p> <p><b>0b0</b></p> <p>DEVPORESETn is not asserted when in DBG_RECOV.</p> <p><b>0b1</b></p> <p>DEVPORESETn is asserted when in DBG_RECOV.</p>	0b0
[0]	WARM_RST_DEVREQEN	<p>Device interface handshake behavior.</p> <p>This bit should not be modified when the PPU is in WARM_RST, or if the PPU is performing a transition, otherwise PPU behavior is <b>UNPREDICTABLE</b>.</p> <p><b>0b0</b></p> <p>The PPU does not perform a device interface handshake when transitioning between ON and WARM_RST.</p> <p><b>0b1</b></p> <p>The PPU performs a device interface handshake when transitioning between ON and WARM_RST.</p>	0b1

Accessibility

Component	Offset	Range
CLUSTERPPU	0x024	None

This interface is accessible as follows:

RW

B.1.2.3.10 CLUSTERPPU\_IMR, Interrupt Mask Register

This register controls the events that assert the interrupt output. Additional event masking controls are in the Additional Interrupt Mask Register (ext-CLUSTERPPU\_AIMR), Input Edge Sensitivity

Register (ext-CLUSTERPPU\_IESR), and the Operating Mode Active Edge Sensitivity Register (ext-CLUSTERPPU\_OPSR).

When an interrupt event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

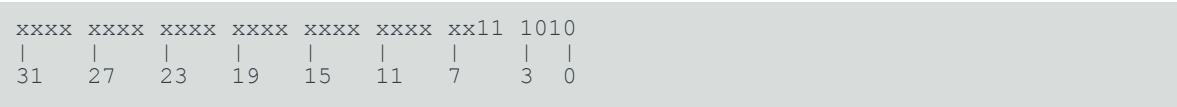
Register offset

0x030

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-79: EXT\_CLUSTERPPU\_IMR bit assignments

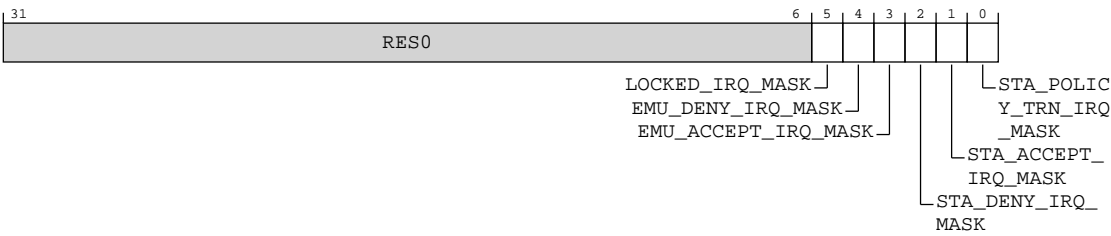


Table B-157: CLUSTERPPU\_IMR bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[5]	LOCKED_IRQ_MASK	Locked event mask  <b>0b0</b> Locked event enabled.  <b>0b1</b> Locked event masked.	0b1
[4]	EMU_DENY_IRQ_MASK	Emulation transition denial event mask  <b>0b0</b> Emulation transition denial event enabled.  <b>0b1</b> Emulation transition denial event masked.	0b1
[3]	EMU_ACCEPT_IRQ_MASK	Emulation transition acceptance event mask  <b>0b0</b> Emulation transition acceptance event enabled.  <b>0b1</b> Emulation transition acceptance event masked.	0b1
[2]	STA_DENY_IRQ_MASK	Static transition denial event mask  <b>0b0</b> Static transition denial event enabled.  <b>0b1</b> Static transition denial event masked.	0b0
[1]	STA_ACCEPT_IRQ_MASK	Static transition acceptance event mask  <b>0b0</b> Static transition acceptance event enabled.  <b>0b1</b> Static transition acceptance event masked.	0b1
[0]	STA_POLICY_TRN_IRQ_MASK	Static full policy transition completion event mask  <b>0b0</b> Static full policy transition completion event enabled.  <b>0b1</b> Static full policy transition completion event masked.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPPU	0x030	None

This interface is accessible as follows:

RW

#### B.1.2.3.11 CLUSTERPPU\_AIMR, Additional Interrupt Mask Register

This register controls the events that assert the interrupt output. Additional event masking controls are in the Interrupt Mask Register (ext-CLUSTERPPU\_IMR), Input Edge Sensitivity Register (ext-CLUSTERPPU\_IISR), and the Operating Mode Active Edge Sensitivity Register (ext-CLUSTERPPU\_OPSR).

When an interrupt event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

## Configurations

This register is available in all configurations.

## Attributes

## Width

32

## Component

## CLUSTERPPU

## Register offset

0x034

### Access type

RW

### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx1	1110
31	27	23	19	15	11	7	3 0

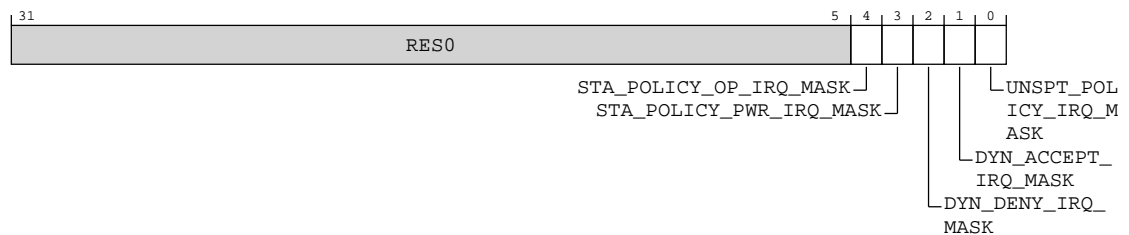


### Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure B-80: EXT\_CLUSTERPPU\_AIMR bit assignments



**Table B-159: CLUSTERPPU\_AIMR bit descriptions**

Bits	Name	Description	Reset
[31:5]	RES0	Reserved	RES0
[4]	STA_POLICY_OP_IRQ_MASK	Static operating policy transition completion event mask  <b>0b0</b> Static operating policy transition completion event enabled. <b>0b1</b> Static operating policy transition completion event masked.	0b1
[3]	STA_POLICY_PWR_IRQ_MASK	Static power policy transition completion event mask  <b>0b0</b> Static power policy transition completion event enabled. <b>0b1</b> Static power policy transition completion event masked.	0b1
[2]	DYN_DENY_IRQ_MASK	Dynamic transition denial event mask  <b>0b0</b> Dynamic transition denial event enabled. <b>0b1</b> Dynamic transition denial event masked.	0b1
[1]	DYN_ACCEPT_IRQ_MASK	Dynamic transition acceptance event mask  <b>0b0</b> Dynamic transition acceptance event enabled. <b>0b1</b> Dynamic transition acceptance event masked.	0b1
[0]	UNSPT_POLICY_IRQ_MASK	Unsupported policy event mask  <b>0b0</b> Unsupported policy event enabled. <b>0b1</b> Unsupported policy event masked.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPPU	0x034	None

This interface is accessible as follows:

RW



B.1.2.3.12 CLUSTERPPU\_ISR, Interrupt Status Register

This register contains information about events causing the assertion of the interrupt output. It is also used to clear interrupt events.

A bit set to 0b1 indicates the event asserted the interrupt output. Multiple events can be active at the same time. When an interrupt event is masked an occurrence of that event does not set the status bit.

A write of 0b1 to an event bit clears that event. A write of 0b0 to a bit has no effect. The interrupt output stays HIGH until all status bits in the Interrupt Status Register (CLUSTERPPU\_ISR) and the Additional Interrupt Status Register (ext-CLUSTERPPU\_AISR) are 0b0.

When the OTHER\_IRQ bit is set, this indicates an event from the Additional Interrupt Status Register (CLUSTERPPU\_AISR) has caused the interrupt output to be asserted. This bit cannot be cleared by writing to this register. It must be cleared by writing to the active event in the Additional Interrupt Status Register (ext-CLUSTERPPU\_AISR).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x038

Access type

RW1C

Reset value

xxxx	xx00	xxxx	x000	xxxx	000x	0x00	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.



Bits	Name	Description	Reset
[15:12]	<b>RES0</b>	Reserved	<b>RES0</b>
[11]	PWR_ACTIVE_EDGE_IRQ3	Indicates if power mode DEVPACTIVE[3] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[3] input (MEM_RET_EMU) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[3] input (MEM_RET_EMU) asserted the interrupt output.	0b0
[10]	PWR_ACTIVE_EDGE_IRQ2	Indicates if power mode DEVPACTIVE[2] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[2] input (MEM_RET) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[2] input (MEM_RET) asserted the interrupt output.	0b0
[9]	PWR_ACTIVE_EDGE_IRQ1	Indicates if power mode DEVPACTIVE[1] input caused the input edge event.  <b>0b0</b> DEVPACTIVE[1] input (OFF_EMU) did not assert the interrupt output.  <b>0b1</b> DEVPACTIVE[1] input (OFF_EMU) asserted the interrupt output.	0b0
[8]	<b>RES0</b>	Reserved	<b>RES0</b>
[7]	OTHER_IRQ	Indicates there is an interrupt event pending in the Additional Interrupt Status Register (ext-CLUSTERPPU_AISR).  <b>0b0</b> No interrupt pending in ext-CLUSTERPPU_AISR.  <b>0b1</b> Interrupt pending in ext-CLUSTERPPU_AISR.	0b0
[6]	<b>RES0</b>	Reserved	<b>RES0</b>
[5]	LOCKED_IRQ	Locked event status.  <b>0b0</b> No locked event.  <b>0b1</b> A locked event asserted the interrupt output.	0b0
[4]	EMU_DENY_IRQ	Emulated transition denial event status.  <b>0b0</b> No emulated transition denial event.  <b>0b1</b> An emulated transition denial event asserted the interrupt output.	0b0
[3]	EMU_ACCEPT_IRQ	Emulated transition acceptance event status.  <b>0b0</b> No emulated transition acceptance event.  <b>0b1</b> An emulated transition acceptance event asserted the interrupt output.	0b0

Bits	Name	Description	Reset
[2]	STA_DENY_IRQ	Static transition denial event status.  <b>0b0</b> No static transition denial event.  <b>0b1</b> An static transition denial event asserted the interrupt output.	0b0
[1]	STA_ACCEPT_IRQ	Static transition acceptance event status.  <b>0b0</b> No static transition acceptance event.  <b>0b1</b> An static transition acceptance event asserted the interrupt output.	0b0
[0]	STA_POLICY_TRN_IRQ	Static full policy transition completion event status.  <b>0b0</b> No static full policy transition completion event.  <b>0b1</b> An static full policy transition completion event asserted the interrupt output.	0b0

## Accessibility

Component	Offset	Range
CLUSTERPPU	0x038	None

This interface is accessible as follows:

RW

### B.1.2.3.13 CLUSTERPPU\_AISR, Additional Interrupt Status Register

This register contains information about events causing the assertion of the interrupt output. It is also used to clear interrupt events.

A bit set to 0b1 indicates the event asserted the interrupt output. Multiple events can be active at the same time. When an interrupt event is masked an occurrence of that event does not set the status bit.

A write of 0b1 to an event bit clears that event. A write of 0b0 has no effect. The interrupt output stays HIGH until all status bits in the Interrupt Status Register (ext-CLUSTERPPU\_ISR) and the Additional Interrupt Status Register (CLUSTERPPU\_AISR) are set to 0b0.

When an interrupt status is set to 0b1 in this register it sets the OTHER\_IRQ bit in the Interrupt Status Register (ext-CLUSTERPPU\_ISR). Status bits in this register are only cleared by writing to this register.

## Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x03C

Access type

RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-82: EXT\_CLUSTERPPU\_AISR bit assignments

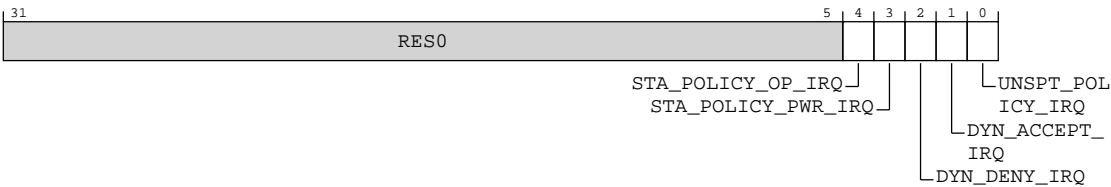


Table B-163: CLUSTERPPU\_AISR bit descriptions

Bits	Name	Description	Reset
[31:5]	RES0	Reserved	RES0
[4]	STA_POLICY_OP_IRQ	Static operating policy transition completion event status  <b>0b0</b> No static operating policy transition completion event.  <b>0b1</b> A static operating policy transition completion event asserted the interrupt output.	0b0
[3]	STA_POLICY_PWR_IRQ	Static power policy transition completion event status  <b>0b0</b> No static power policy transition completion event.  <b>0b1</b> A static power policy transition completion event asserted the interrupt output.	0b0

Bits	Name	Description	Reset
[2]	DYN_DENY_IRQ	Dynamic transition denial event status  <b>0b0</b> No dynamic transition denial event.  <b>0b1</b> A dynamic transition denial event asserted the interrupt output.	0b0
[1]	DYN_ACCEPT_IRQ	Dynamic transition acceptance event status  <b>0b0</b> No dynamic transition acceptance event.  <b>0b1</b> A dynamic transition acceptance event asserted the interrupt output.	0b0
[0]	UNSPT_POLICY_IRQ	Unsupported policy event status  <b>0b0</b> No unsupported policy event.  <b>0b1</b> An unsupported policy event asserted the interrupt output.	0b0

## Accessibility

Component	Offset	Range
CLUSTERPPU	0x03C	None

This interface is accessible as follows:

RW

### B.1.2.3.14 CLUSTERPPU\_IESR, Input Edge Sensitivity Register

This register configures the transitions on the power mode DEVPACTIVE inputs that generate an Input Edge interrupt event.

When an event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

CLUSTERPPU

### Register offset

0x040

Access type

RW

Reset value

xxxx	xxxx	xx00	0000	0000	0000	0000	00xx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-83: EXT\_CLUSTERPPU\_IESR bit assignments

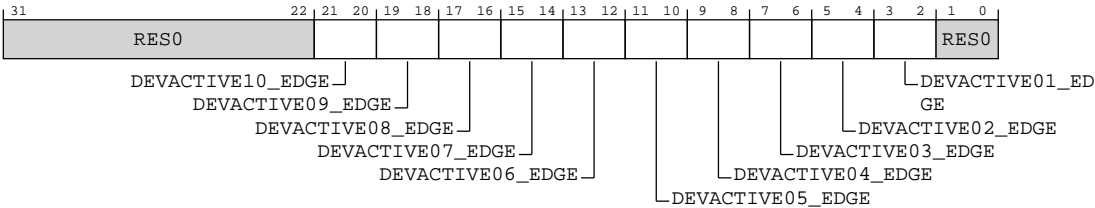


Table B-165: CLUSTERPPU\_IESR bit descriptions

Bits	Name	Description	Reset
[31:22]	RES0	Reserved	RES0
[21:20]	DEVACTIVE10_EDGE	Configures the transitions on the DEVPACTIVE[10] input (DBG_RECOV) that generate an Input Edge interrupt event.  <b>0b00</b> Event maksed.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00

Bits	Name	Description	Reset
[19:18]	DEVACTIVE09_EDGE	<p>Configures the transitions on the DEVPACTIVE[9] input (WARM_RST) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[17:16]	DEVACTIVE08_EDGE	<p>Configures the transitions on the DEVPACTIVE[8] input (ON) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[15:14]	DEVACTIVE07_EDGE	<p>Configures the transitions on the DEVPACTIVE[7] input (unused) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[13:12]	DEVACTIVE06_EDGE	<p>Configures the transitions on the DEVPACTIVE[6] input (unused) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00



Bits	Name	Description	Reset
[11:10]	DEVACTIVE05_EDGE	<p>Configures the transitions on the DEVPACTIVE[5] input (unused) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[9:8]	DEVACTIVE04_EDGE	<p>Configures the transitions on the DEVPACTIVE[4] input (unused) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[7:6]	DEVACTIVE03_EDGE	<p>Configures the transitions on the DEVPACTIVE[3] input (MEM_RET_EMU) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00
[5:4]	DEVACTIVE02_EDGE	<p>Configures the transitions on the DEVPACTIVE[2] input (MEM_RET) that generate an Input Edge interrupt event.</p> <p><b>0b00</b> Event masked.</p> <p><b>0b01</b> Rising edge of event generates an interrupt.</p> <p><b>0b10</b> Falling edge of event generates an interrupt.</p> <p><b>0b11</b> Both edges of event generate an interrupt.</p>	0b00

Bits	Name	Description	Reset
[3:2]	DEVACTIVE01_EDGE	Configures the transitions on the DEVPACTIVE[1] input (OFF_EMU) that generate an Input Edge interrupt event.  <b>0b00</b> Event maksed.  <b>0b01</b> Rising edge of event generates an interrupt.  <b>0b10</b> Falling edge of event generates an interrupt.  <b>0b11</b> Both edges of event generate an interrupt.	0b00
[1:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x040	None

This interface is accessible as follows:

RW

B.1.2.3.15 CLUSTERPPU\_OPSR, Operating Mode Active Edge Sensitivity Register

This register configures the transitions on the operating mode DEVPACTIVE inputs that generate an Input Edge interrupt event.

When an event is masked an occurrence of the event does not set the corresponding bit in the interrupt status register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x044

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
------	------	------	------	------	------	------	------



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-84: EXT\_CLUSTERPPU\_OPSR bit assignments

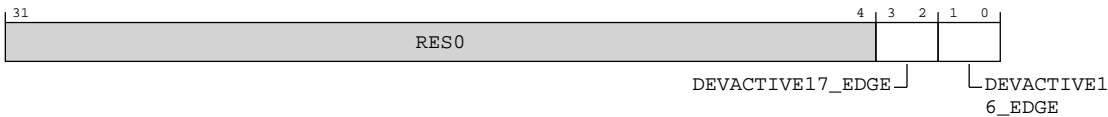


Table B-167: CLUSTERPPU\_OPSR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:2]	DEVACTIVE17_EDGE	Configures the transitions on the DEVPACTIVE[17] input (OPMODE_02) that generate an Input Edge interrupt event.  0b00 Event maksed.  0b01 Rising edge of event generates an interrupt.  0b10 Falling edge of event generates an interrupt.  0b11 Both edges of event generate an interrupt.	0b00
[1:0]	DEVACTIVE16_EDGE	Configures the transitions on the DEVPACTIVE[16] input (OPMODE_01) that generate an Input Edge interrupt event.  0b00 Event maksed.  0b01 Rising edge of event generates an interrupt.  0b10 Falling edge of event generates an interrupt.  0b11 Both edges of event generate an interrupt.	0b00

Accessibility

Component	Offset	Range
CLUSTERPPU	0x044	None

This interface is accessible as follows:

RW

B.1.2.3.16 CLUSTERPPU\_FUNRR, Functional Retention RAM Configuration Register

This register is reserved.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

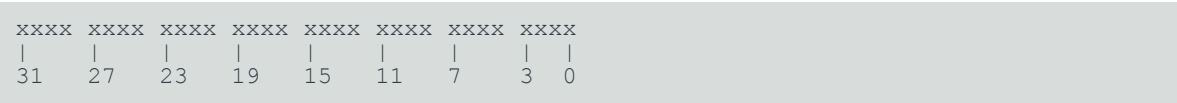
Register offset

0x050

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-85: EXT\_CLUSTERPPU\_FUNRR bit assignments

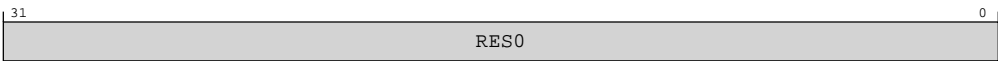


Table B-169: CLUSTERPPU\_FUNRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x050	None

This interface is accessible as follows:

RW

B.1.2.3.17 CLUSTERPPU\_FULRR, Full Retention RAM Configuration Register

This register is reserved (high bits of PCSMPSTATE outputs are not configurable by software).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

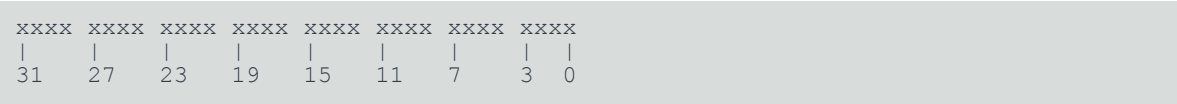
Register offset

0x054

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-86: EXT\_CLUSTERPPU\_FULRR bit assignments

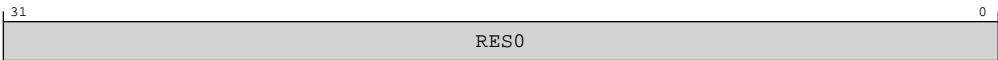


Table B-171: CLUSTERPPU\_FULRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x054	None

This interface is accessible as follows:

RW

B.1.2.3.18 CLUSTERPPU\_MEMRR, Memory Retention RAM Configuration Register

This register is reserved (high bits of PCSMPSTATE outputs are not configurable by software).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0x058

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-87: EXT\_CLUSTERPPU\_MEMRR bit assignments

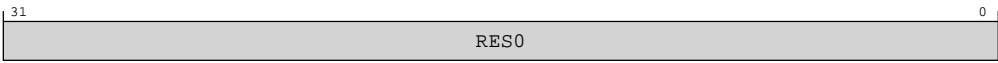


Table B-173: CLUSTERPPU\_MEMRR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x058	None

This interface is accessible as follows:

RW

B.1.2.3.19 CLUSTERPPU\_EDTR0, Power Mode Entry Delay Register 0

This register is reserved (power mode entry delays not supported).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

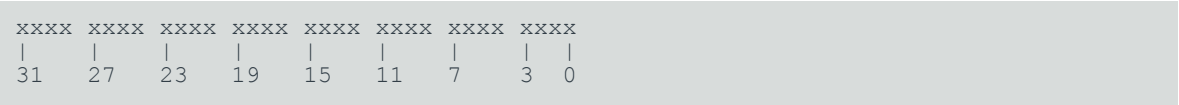
Register offset

0x160

Access type

RW

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-88: EXT\_CLUSTERPPU\_EDTR0 bit assignments

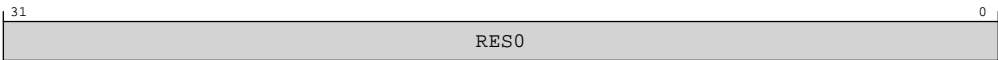


Table B-175: CLUSTERPPU\_EDTR0 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x160	None

This interface is accessible as follows:

RW

B.1.2.3.20 CLUSTERPPU\_EDTR1, Power Mode Entry Delay Register 1

This register is reserved (power mode entry delays not supported).

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

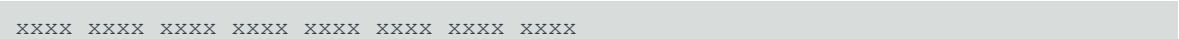
Register offset

0x164

Access type

RW

Reset value







Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-89: EXT\_CLUSTERPPU\_EDTR1 bit assignments

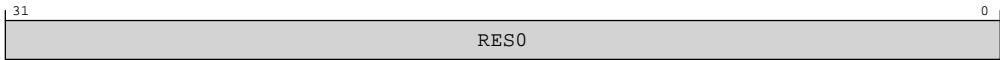


Table B-177: CLUSTERPPU\_EDTR1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0x164	None

This interface is accessible as follows:

RW

B.1.2.3.21 CLUSTERPPU\_DCDR0, Device Control Delay Configuration Register 0

This register is used to program device control delay parameters.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

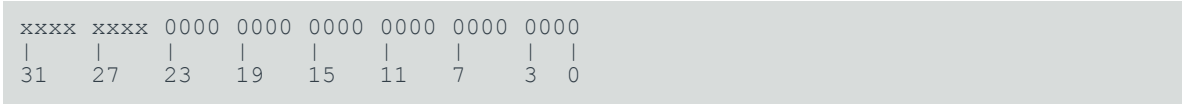
Register offset

0x170

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-90: EXT\_CLUSTERPPU\_DCDR0 bit assignments

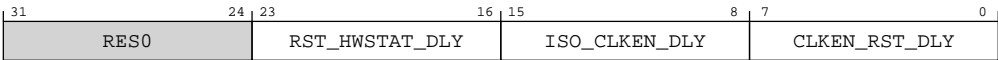


Table B-179: CLUSTERPPU\_DCDR0 bit descriptions

Bits	Name	Description	Reset
[31:24]	RES0	Reserved	RES0
[23:16]	RST_HWSTAT_DLY	Delay from reset de-assertion to HWSTAT update.	0x00
[15:8]	ISO_CLKEN_DLY	Delay from isolation enable de-assertion to clock enable assertion.	0x00
[7:0]	CLKEN_RST_DLY	Delay from clock enable assertion to reset de-assertion.	0x00

Accessibility

Component	Offset	Range
CLUSTERPPU	0x170	None

This interface is accessible as follows:

RW

B.1.2.3.22 CLUSTERPPU\_DCDR1, Device Control Delay Configuration Register 1

This register is used to program device control delay parameters.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

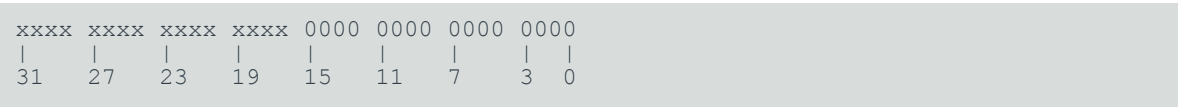
Register offset

0x174

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-91: EXT\_CLUSTERPPU\_DCDR1 bit assignments

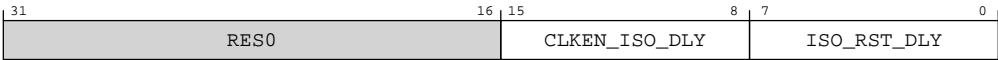


Table B-181: CLUSTERPPU\_DCDR1 bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0
[15:8]	CLKEN_ISO_DLY	Delay from clock enable de-assertion to isolation enable assertion.	0x00
[7:0]	ISO_RST_DLY	Delay from isolation enable assertion to reset assertion.	0x00

Accessibility

Component	Offset	Range
CLUSTERPPU	0x174	None

This interface is accessible as follows:

RW

### B.1.2.3.23 CLUSTERPPU\_IDR0, PPU Identification Register 0

This read-only register contains information on the type and number of channels on the device interface and power and operating modes supported.

Additional information on optional features can be found in the PPU Identification Register 1 (ext-CLUSTERPPU\_IDR1).

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

CLUSTERPPU

### Register offset

0xFB0

### Access type

RO

### Reset value

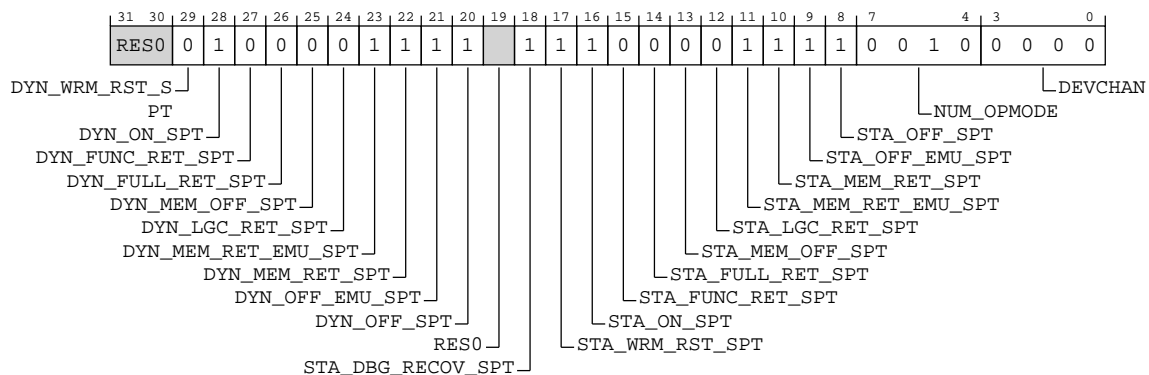
xx01	0000	1111	x111	0000	1111	0010	0000
31	27	23	19	15	11	7	3
							0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-92: EXT\_CLUSTERPPU\_IDR0 bit assignments



**Table B-183: CLUSTERPPU\_IDR0 bit descriptions**

Bits	Name	Description	Reset
[31:30]	<b>RES0</b>	Reserved	<b>RES0</b>
[29]	DYN_WRM_RST_SPT	Dynamic WARM_RST support. <b>0b0</b> Dynamic WARM_RST not supported.	0b0
[28]	DYN_ON_SPT	Dynamic ON support. <b>0b1</b> Dynamic ON supported.	0b1
[27]	DYN_FUNC_RET_SPT	Dynamic DYN_FUNC_RET_SPT support. <b>0b0</b> Dynamic DYN_FUNC_RET_SPT not supported.	0b0
[26]	DYN_FULL_RET_SPT	Dynamic DYN_FULL_RET_SPT support. <b>0b0</b> Dynamic DYN_FULL_RET_SPT not supported.	0b0
[25]	DYN_MEM_OFF_SPT	Dynamic MEM_OFF support. <b>0b0</b> Dynamic MEM_OFF not supported.	0b0
[24]	DYN_LGC_RET_SPT	Dynamic LOGIC_RET support. <b>0b0</b> Dynamic LOGIC_RET not supported.	0b0
[23]	DYN_MEM_RET_EMU_SPT	Dynamic DYN_MEM_RET_EMU_SPT support. <b>0b1</b> Dynamic DYN_MEM_RET_EMU_SPT supported.	0b1
[22]	DYN_MEM_RET_SPT	Dynamic DYN_MEM_RET_SPT support. <b>0b1</b> Dynamic DYN_MEM_RET_SPT supported.	0b1
[21]	DYN_OFF_EMU_SPT	Dynamic OFF_EMU support. <b>0b1</b> Dynamic OFF_EMU supported.	0b1
[20]	DYN_OFF_SPT	Dynamic OFF support. <b>0b1</b> Dynamic OFF supported.	0b1
[19]	<b>RES0</b>	Reserved	<b>RES0</b>
[18]	STA_DBG_RECOV_SPT	DBG_RECOV support. <b>0b1</b> DBG_RECOV supported.	0b1
[17]	STA_WRM_RST_SPT	WRM_RST support. <b>0b1</b> WRM_RST supported.	0b1

Bits	Name	Description	Reset
[16]	STA_ON_SPT	ON support. <b>0b1</b> ON supported.	0b1
[15]	STA_FUNC_RET_SPT	FUNC_RET support. <b>0b0</b> FUNC_RET not supported.	0b0
[14]	STA_FULL_RET_SPT	FULL_RET support. <b>0b0</b> FULL_RET not supported.	0b0
[13]	STA_MEM_OFF_SPT	MEM_OFF support. <b>0b0</b> MEM_OFF not supported.	0b0
[12]	STA_LGC_RET_SPT	LOGIC_RET support. <b>0b0</b> LOGIC_RET not supported.	0b0
[11]	STA_MEM_RET_EMU_SPT	MEM_RET_EMU support. <b>0b1</b> MEM_RET_EMU supported.	0b1
[10]	STA_MEM_RET_SPT	MEM_RET support. <b>0b1</b> MEM_RET supported.	0b1
[9]	STA_OFF_EMU_SPT	OFF_EMU support. <b>0b1</b> OFF_EMU supported.	0b1
[8]	STA_OFF_SPT	OFF support. <b>0b1</b> OFF supported.	0b1
[7:4]	NUM_OPMODE	No. of operating modes supported, minus 1. <b>0b0010</b> 3 operating modes supported.	0b0010
[3:0]	DEVCHAN	No. of Device Interface Channels. <b>0b0000</b> 0 (P-channel PPU).	0b0000

### Accessibility

Component	Offset	Range
CLUSTERPPU	0xFB0	None

This interface is accessible as follows:

RO

### B.1.2.3.24 CLUSTERPPU\_IDR1, PPU Identification Register 1

This read-only register contains information on the optional features and configurations that are supported by this CLUSTERPPU.

Additional information on optional features can be found in the PPU Identification Register 0 (ext-CLUSTERPPU\_IDR0).

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

CLUSTERPPU

### Register offset

0xFB4

### Access type

RO

### Reset value

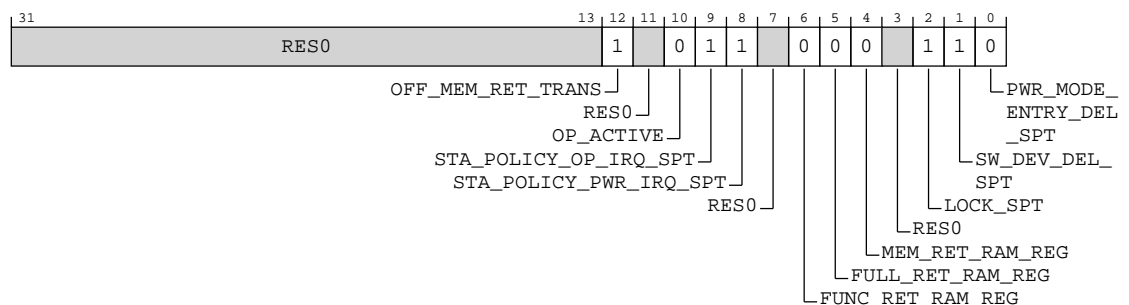
xxxx	xxxx	xxxx	xxxx	xxx1	x011	x000	x110
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-93: EXT\_CLUSTERPPU\_IDR1 bit assignments



**Table B-185: CLUSTERPPU\_IDR1 bit descriptions**

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0
[12]	OFF_MEM_RET_TRANS	OFF to MEM_RET direct transition. Indicates if direct transitions from OFF to MEM_RET and from OFF_EMU to MEM_RET_EMU are supported.  <b>0b1</b> OFF to MEM_RET direct transition supported.	0b1
[11]	RES0	Reserved	RES0
[10]	OP_ACTIVE	Operating mode use model for dynamic transitions.  <b>0b0</b> Ladder use model.	0b0
[9]	STA_POLICY_OP_IRQ_SPT	Operating policy transition completion event status.  <b>0b1</b> Operating policy transition completion events supported.	0b1
[8]	STA_POLICY_PWR_IRQ_SPT	Power policy transition completion event status.  <b>0b1</b> Power policy transition completion events supported.	0b1
[7]	RES0	Reserved	RES0
[6]	FUNC_RET_RAM_REG	Indicates if the ext-CLUSTERPPU_FUNRR register is present or reserved.  <b>0b0</b> ext-CLUSTERPPU_FUNRR is reserved.	0b0
[5]	FULL_RET_RAM_REG	Indicates if the ext-CLUSTERPPU_FULRR register is present or reserved.  <b>0b0</b> ext-CLUSTERPPU_FULRR is reserved.	0b0
[4]	MEM_RET_RAM_REG	Indicates if the ext-CLUSTERPPU_MEMRR register is present or reserved.  <b>0b0</b> ext-CLUSTERPPU_MEMRR is not present.	0b0
[3]	RES0	Reserved	RES0
[2]	LOCK_SPT	Indicates if the lock and the lock interrupt event are supported.  <b>0b1</b> Lock and the lock interrupt event are supported.	0b1
[1]	SW_DEV_DEL_SPT	Software device delay control configuration support.  <b>0b1</b> Software device delay control configuration supported.	0b1
[0]	PWR_MODE_ENTRY_DEL_SPT	Power mode entry delay support.  <b>0b0</b> Power mode entry delay not supported.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPPU	0xFB4	None

This interface is accessible as follows:



RO

B.1.2.3.25 CLUSTERPPU\_IIDR, Implementation Identification Register

This register provides information about the implementer and implementation of the PPU.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFC8

Access type

RO

Reset value

0000 1011 0110 0001 0001 0100 0011 1011

Bit descriptions

Figure B-94: EXT\_CLUSTERPPU\_IIDR bit assignments

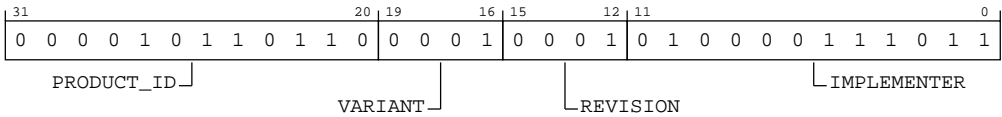


Table B-187: CLUSTERPPU\_IIDR bit descriptions

Bits	Name	Description	Reset
[31:20]	PRODUCT_ID	Value identifying the PPU part.  0b000010110110 PCK-600 PPU.	0x0B6
[19:16]	VARIANT	Value used to distinguish product variants, or major revisions of the product.  0b0001 Product variant r0p5.	0b0001
[15:12]	REVISION	Value used to distinguish minor revisions of the product.  0b0001 No ECO fixes.	0b0001

Bits	Name	Description	Reset
[11:0]	IMPLEMENTER	Implementer identification.  <b>0b010000111011</b> Arm Limited.	0x43B

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFC8	None

This interface is accessible as follows:

RO

B.1.2.3.26 CLUSTERPPU\_AIDR, Architecture Identification Register

This register identifies the PPU architecture revision.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFCC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0001
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-95: EXT\_CLUSTERPPU\_AIDR bit assignments

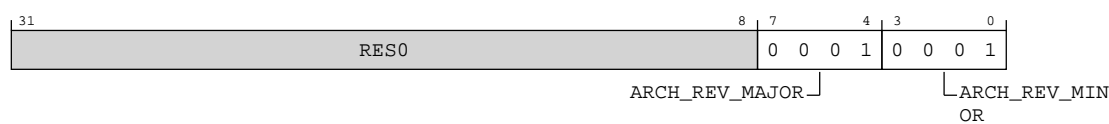


Table B-189: CLUSTERPPU\_AIDR bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	ARCH_REV_MAJOR	PPU architecture major revision.  0b0001 PPU architecture major revision 1.	0b0001
[3:0]	ARCH_REV_MINOR	PPU architecture minor revision.  0b0001 PPU architecture minor revision 1.	0b0001

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFCC	None

This interface is accessible as follows:

RO

B.1.2.3.27 CLUSTERPPU\_PIDR4, PPU Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

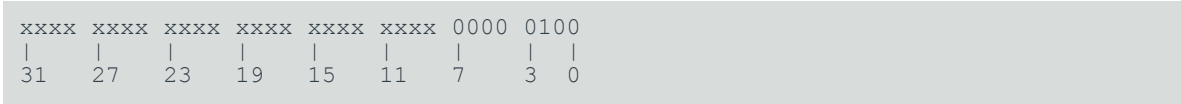
Register offset

0xFD0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-96: EXT\_CLUSTERPPU\_PIDR4 bit assignments



Table B-191: CLUSTERPPU\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count. <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code. <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFD0	None

This interface is accessible as follows:

RO

B.1.2.3.28 CLUSTERPPU\_PIDR5, PPU Peripheral Identification Register 5

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFD4

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-97: EXT\_CLUSTERPPU\_PIDR5 bit assignments

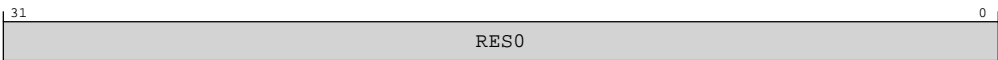


Table B-193: CLUSTERPPU\_PIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFD4	None

This interface is accessible as follows:

RO

B.1.2.3.29 CLUSTERPPU\_PIDR6, PPU Peripheral Identification Register 6

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFD8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-98: EXT\_CLUSTERPPU\_PIDR6 bit assignments

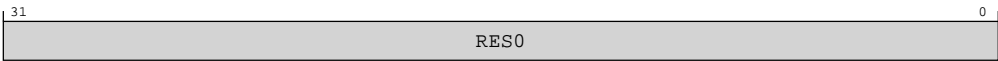


Table B-195: CLUSTERPPU\_PIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFD8	None

This interface is accessible as follows:

RO

B.1.2.3.30 CLUSTERPPU\_PIDR7, PPU Peripheral Identification Register 7

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFDC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-99: EXT\_CLUSTERPPU\_PIDR7 bit assignments

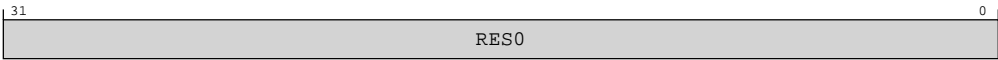


Table B-197: CLUSTERPPU\_PIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFDC	None

This interface is accessible as follows:

RO

B.1.2.3.31 CLUSTERPPU\_PIDR0, PPU Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFE0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-100: EXT\_CLUSTERPPU\_PIDR0 bit assignments

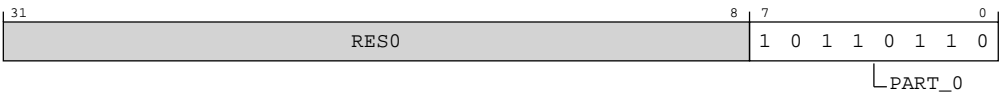


Table B-199: CLUSTERPPU\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[7:0]	PART_0	Part number bits [7:0].  <b>0b10110110</b> PCK-600 PPU. Bits [7:0] of part number 0x0B6.	0xB6

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFE0	None

This interface is accessible as follows:

RO

B.1.2.3.32 CLUSTERPPU\_PIDR1, PPU Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFE4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-101: EXT\_CLUSTERPPU\_PIDR1 bit assignments



Table B-201: CLUSTERPPU\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0].  0b1011 Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8].  0b0000 PCK-600 PPU. Bits [11:8] of part number 0x0B6.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFE4	None

This interface is accessible as follows:

RO

B.1.2.3.33 CLUSTERPPU\_PIDR2, PPU Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-102: EXT\_CLUSTERPPU\_PIDR2 bit assignments

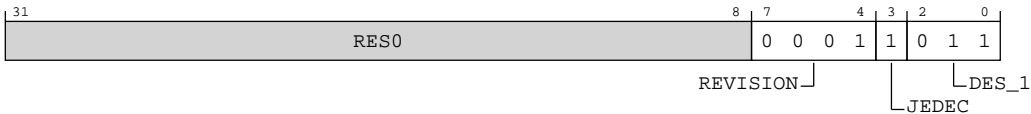


Table B-203: CLUSTERPPU\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision. <b>0b0001</b> Revision r0p5.	0b0001
[3]	JEDEC	JEDEC assignee. <b>0b1</b> JEDEC-assignee values is used.	0b1
[2:0]	DES_1	JEP106 identification code bits [6:4]. <b>0b011</b> Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFE8	None

This interface is accessible as follows:

RO

B.1.2.3.34 CLUSTERPPU\_PIDR3, PPU Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFEC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-103: EXT\_CLUSTERPPU\_PIDR3 bit assignments

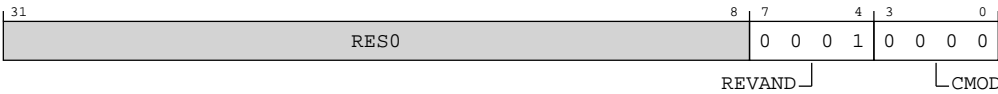


Table B-205: CLUSTERPPU\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes.  0b0001 No ECO fixes.	0b0001
[3:0]	CMOD	Customer Modified.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFEC	None

This interface is accessible as follows:

RO

B.1.2.3.35 CLUSTERPPU\_CIDR0, CLUSTERPPU Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFF0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	1101
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-104: EXT\_CLUSTERPPU\_CIDR0 bit assignments



Table B-207: CLUSTERPPU\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble.  0b00001101 CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFF0	None

This interface is accessible as follows:

RO

B.1.2.3.36 CLUSTERPPU\_CIDR1, CLUSTERPPU Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFF4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1111	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-105: EXT\_CLUSTERPPU\_CIDR1 bit assignments

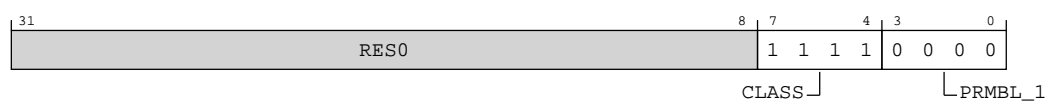


Table B-209: CLUSTERPPU\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1111</b> CoreLink component.	0b1111
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFF4	None

This interface is accessible as follows:

RO

B.1.2.3.37 CLUSTERPPU\_CIDR2, CLUSTERPPU Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPPU

Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-106: EXT\_CLUSTERPPU\_CIDR2 bit assignments



Table B-211: CLUSTERPPU\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble.  0b000000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFF8	None

This interface is accessible as follows:

RO

B.1.2.3.38 CLUSTERPPU\_CIDR3, CLUSTERPPU Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32



Component

CLUSTERPPU

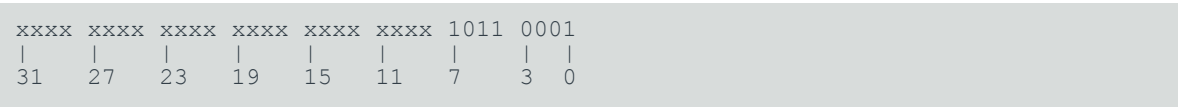
Register offset

0xFFC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-107: EXT\_CLUSTERPPU\_CIDR3 bit assignments



Table B-213: CLUSTERPPU\_CIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble. <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
CLUSTERPPU	0xFFC	None

This interface is accessible as follows:

RO

B.1.2.4 External Cluster Safety register description

This section includes the register descriptions for all External Cluster Safety registers that are accessed for each core.

B.1.2.4.1 CLUSTERSAFETY\_WRITEKEY, PPU Write Key Register

Key register to enable PPU writes. Software must write a specific value to this register before a subsequent write to a PPU register, otherwise the write to the PPU register is ignored. If the subsequent Utility Bus write access is not to a PPU register, a new key write is required.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERSAFETY

Register offset

0x060

Access type

RESERVEDW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-108: EXT\_CLUSTERSAFETY\_WRITEKEY bit assignments



Table B-215: CLUSTERSAFETY\_WRITEKEY bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:0]	KEY	Write protection key. The value 8'hBA must be written to the field to enable a subsequent write to any PPU registers.	0x00

Accessibility

Component	Offset	Range
CLUSTERSAFETY	0x060	None

This interface is accessible as follows:

WO

B.1.2.5 External SBISTC register description

This section includes the register descriptions for all External SBISTC registers that are accessed for each core.

B.1.2.5.1 SBISTC\_FCTLR, Fault Control Register

Sets up the SBIST test and communicates the current status of the test.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0x000

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-109: EXT\_SBISTC\_FCTLR bit assignments

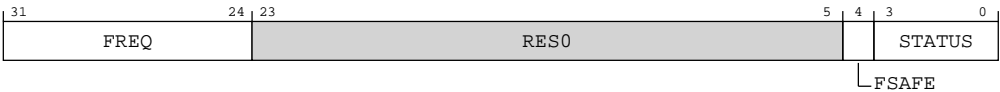


Table B-217: SBISTC\_FCTLR bit descriptions

Bits	Name	Description	Reset
[31:24]	FREQ	Deadlock count x 256. Deadlock count is the programmed value + 1. For example, if the programmed value is 0x1, then the deadlock counter triggers after 512 cycles of inactivity. A maximum deadlock count of 65536 cycles is supported. If the programmed value is 0x0, no deadlock counting will be started unless the counter is activated with DLRESET == 1.	8 {x} <sup>29</sup>
[23:5]	RES0	Reserved	RES0
[4]	FSAFE	This field is used to control failsafe behavior on failure.  <b>0b0</b> Stop and enter low power mode on a detected failure  <b>0b1</b> Return to caller after detecting a failure.	0b0
[3:0]	STATUS	This field is used to control the flow of the SBIST test. The options are:  <b>0b0000</b> IDLE. Currently, there are no tests running.  <b>0b0001</b> INIT. A new test is starting. INIT enables internal checks and sets up other memory mapped registers.  <b>0b0010</b> PING. The test is active and has refreshed the deadlock count.  <b>0b0011</b> DONE. The test library has completed successfully without detecting a fault (all partitions have completed).  <b>0b0100</b> FAIL. An SBIST test or SBIST controller detects a fault.  <b>0b0101</b> PDONE. A test has completed without detecting a fault.  All other values are reserved.  <b>Note:</b> The failure modes must fall within one of the defined categories. The SBIST routine cannot identify a fault that is outside the defined scope of failure modes.	xxxx

<sup>29</sup> If the DLRESET configuration pin is HIGH, this field resets to the value of DLCYCLES configuration pin. Otherwise, this field resets to 0x0 on a Cold reset.

Accessibility

Component	Offset	Range
SBISTC	0x000	None

This interface is accessible as follows:

RO

B.1.2.5.2 SBISTC\_FPIR, Fault Partition Identifier Register

Records the currently running part and also the running iteration of the part in the SBIST test suite.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0x004

Access type

RO

Reset value

xx00	0000	xx00	0000	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-110: EXT\_SBISTC\_FPIR bit assignments

31	30	29	24	23	22	21	16	15	8	7	0
RES0			MTID			RES0	STID		RES0		ITER

Table B-219: SBISTC\_FPIR bit descriptions

Bits	Name	Description	Reset
[31:30]	RES0	Reserved	RES0
[29:24]	MTID	Main Test ID. The SBIST test uses this field to provide an indication of the ID of the main test.	0b000000
[23:22]	RES0	Reserved	RES0
[21:16]	STID	Sub Test ID. The SBIST test uses this field to provide an indication of the ID of the sub test.	0b000000
[15:8]	RES0	Reserved	RES0
[7:0]	ITER	This field is used to indicate the current iteration of the (MTID, STID) combination. If a part is set up to run 'i' iterations, then the programmed value in FPIR.ITER ranges from 0 to i-1.	0x00

Accessibility

Component	Offset	Range
SBISTC	0x004	None

This interface is accessible as follows:

RO

B.1.2.5.3 SBISTC\_FFMIR, Fault Failure Mode Identification Register

Identifies the nature of the fault detected by SBIST. It cannot accurately determine the cause or the point of failure, but it determines the possible nature of the failure mode of the processor.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0x008

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-111: EXT\_SBISTC\_FFMIR bit assignments

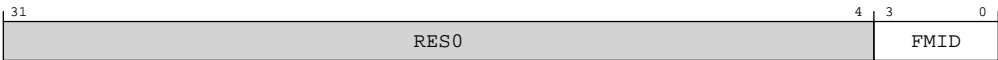


Table B-221: SBISTC\_FFMIR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	FMID	<div>Failure Mode ID. The options are:</div> <div><b>0b0000</b> Not Valid. The contents of this register are not valid. This ID indicates that the register is not yet updated or there is no source to update this register.</div> <div><b>0b0001</b> Deadlock. The test did not make any progress in the time stipulated by the AArch64.IMP_FCTLR_EL1.</div> <div><b>0b0010</b> Exception. The test failed because of an unexpected exception. A failure to take an exception is also categorized using this failure mode.</div> <div><b>0b0011</b> PMU. The test failed because of unexpected events or missing events detected by the PMU.</div> <div><b>0b0100</b> Data corruption. The test has detected a fault because of data corruption.</div> <div>All other values are reserved.</div>	0b0000

Accessibility

Component	Offset	Range
SBISTC	0x008	None

This interface is accessible as follows:

RO

B.1.2.5.4 SBISTC\_DEVARCH, Device Architecture Register

Identifies the architect and architecture of a CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFBC

Access type

RO

Reset value

0100 0111 0111 0000 0000 1010 0101 1000

Bit descriptions

Figure B-112: EXT\_SBISTC\_DEVARCH bit assignments

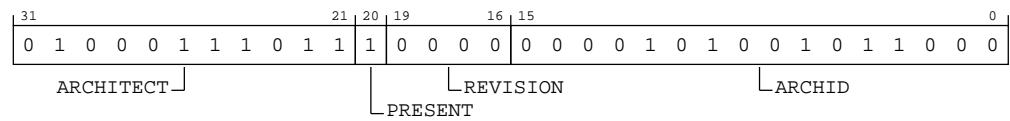


Table B-223: SBISTC\_DEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect. <b>0b01000111011</b> JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	Present. <b>0b1</b> DEVARCH information present.	0b1
[19:16]	REVISION	Revision. <b>0b0000</b> Revision 0.	0b0000
[15:0]	ARCHID	Architecture ID. <b>0b00000101001011000</b> SBIST Controller.	0x0A58



Accessibility

Component	Offset	Range
SBISTC	0xFBC	None

This interface is accessible as follows:

RO

B.1.2.5.5 SBISTC\_IIDR, Implementation Identification Register

Provides information about the implementer and implementation of the SBIST Controller.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFC8

Access type

RO

Reset value

1101 0001 0100 0111 0000 0100 0011 1011

Bit descriptions

Figure B-113: EXT\_SBISTC\_IIDR bit assignments

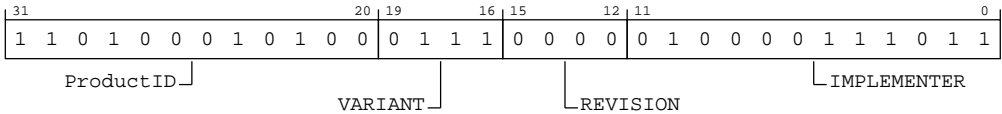


Table B-225: SBISTC\_IIDR bit descriptions

Bits	Name	Description	Reset
[31:20]	ProductID	Part number. <b>0b110100010100</b> Cortex-R82AE SBIST Controller component.	0xD14

Bits	Name	Description	Reset
[19:16]	VARIANT	Value used to distinguish product variants, or major revisions of the product.  <b>0b0111</b> Product variant 7.	0b0111
[15:12]	REVISION	Value used to distinguish minor revisions of the product.  <b>0b0000</b> No ECO fixes.	0b0000
[11:0]	IMPLEMENTER	Implementer identification.  <b>0b010000111011</b> Arm Limited.	0x43B

Accessibility

Component	Offset	Range
SBISTC	0xFC8	None

This interface is accessible as follows:

RO

B.1.2.5.6 SBISTC\_PIDR4, Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFD0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-114: EXT\_SBISTC\_PIDR4 bit assignments



Table B-227: SBISTC\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count.  0b0000 The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code.  0b0100 Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
SBISTC	0xFD0	None

This interface is accessible as follows:

RO

B.1.2.5.7 SBISTC\_PIDR0, Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFE0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-115: EXT\_SBISTC\_PIDR0 bit assignments



Table B-229: SBISTC\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b00010100 Cortex-R82AE SBIST Controller component. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Range
SBISTC	0xFE0	None

This interface is accessible as follows:

RO

B.1.2.5.8 SBISTC\_PIDR1, Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFE4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-116: EXT\_SBISTC\_PIDR1 bit assignments



Table B-231: SBISTC\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0]. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b1101</b> Cortex-R82AE SBIST Controller component. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Range
SBISTC	0xFE4	None

This interface is accessible as follows:

RO

B.1.2.5.9 SBISTC\_PIDR2, Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

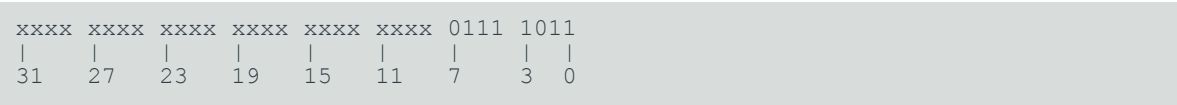
Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-117: EXT\_SBISTC\_PIDR2 bit assignments

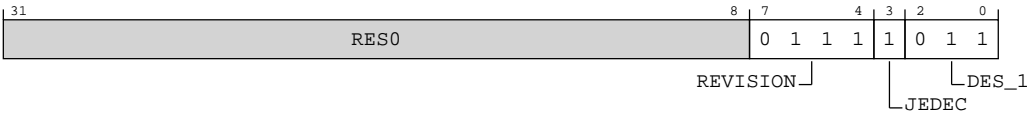


Table B-233: SBISTC\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111

Bits	Name	Description	Reset
[3]	JEDEC	<b>RAO</b> . Indicates a JEP106 identity code is used.  <b>0b1</b> JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  <b>0b011</b> Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
SBISTC	0xFE8	None

This interface is accessible as follows:

RO

B.1.2.5.10 SBISTC\_PIDR3, Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFE8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-118: EXT\_SBISTC\_PIDR3 bit assignments

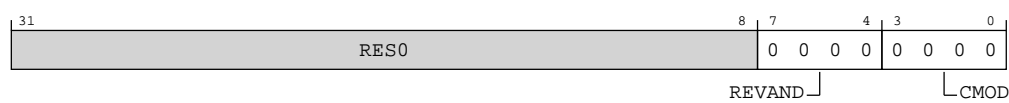


Table B-235: SBISTC\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes. <b>0b0000</b> No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified. <b>0b0000</b> The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
SBISTC	0xFEC	None

This interface is accessible as follows:

RO

B.1.2.5.11 SBISTC\_CIDR0, Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

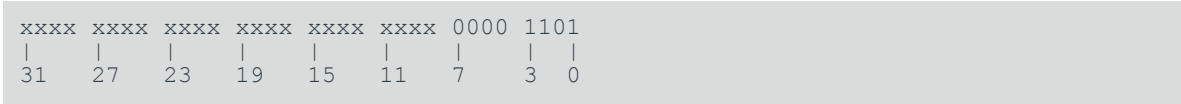
0xFF0

Access type

RO



Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-119: EXT\_SBISTC\_CIDR0 bit assignments

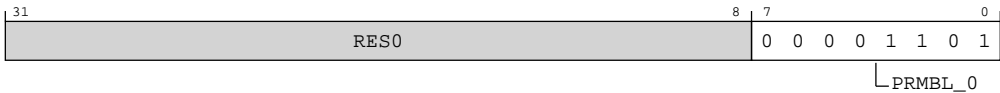


Table B-237: SBISTC\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble. <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
SBISTC	0xFF0	None

This interface is accessible as follows:

RO

B.1.2.5.12 SBISTC\_CIDR1, Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

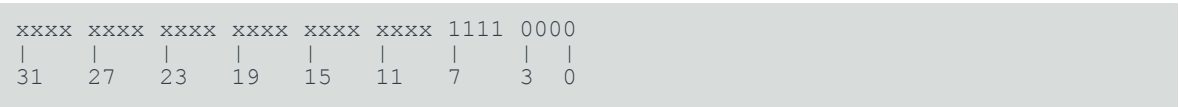
Register offset

0xFF4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-120: EXT\_SBISTC\_CIDR1 bit assignments

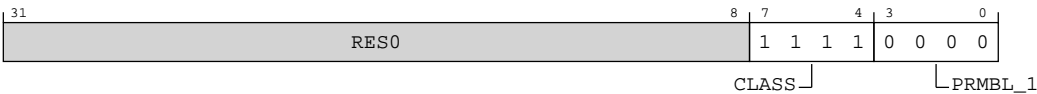


Table B-239: SBISTC\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1111</b> CoreLink component.	0b1111
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
SBISTC	0xFF4	None

This interface is accessible as follows:

RO

B.1.2.5.13 SBISTC\_CIDR2, Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

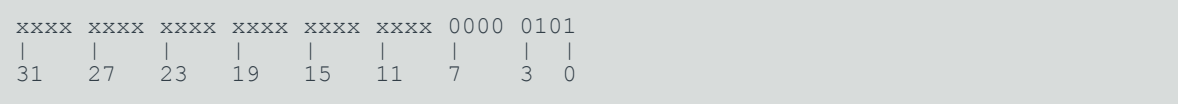
Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-121: EXT\_SBISTC\_CIDR2 bit assignments

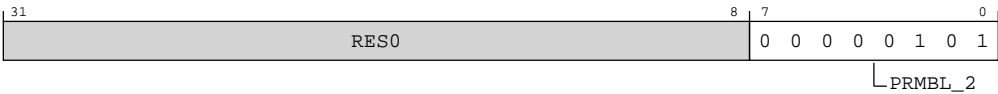


Table B-241: SBISTC\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble.  0b000000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
SBISTC	0xFF8	None

This interface is accessible as follows:

RO

B.1.2.5.14 SBISTC\_CIDR3, Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

SBISTC

Register offset

0xFFC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0001
31	27	23	19	15	11	7	3 0

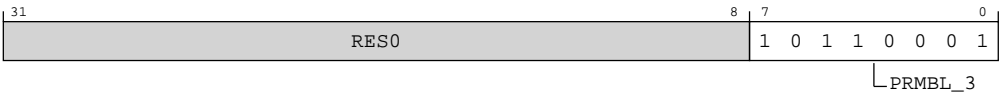


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-122: EXT\_SBISTC\_CIDR3 bit assignments



**Table B-243: SBISTC\_CIDR3 bit descriptions**

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble.  <b>0b10110001</b> CoreSight component identification preamble.	0xB1

### Accessibility

Component	Offset	Range
SBISTC	0xFFC	None

This interface is accessible as follows:

RO

## B.2 Registers accessed over the Debug APB bus

This section contains the summary and descriptions for all the external registers in the Cortex®-R82AE processor accessed over the Debug APB bus.

Debug APB bus implements one of two memory maps:

- A sparse memory map, when the configuration parameter `DENSE_CS_ADDR_MAP` is 0. Each set of System registers is grouped on separate 64KB page boundaries. This allows to isolate and remap components when using the EL1 MMU (if VMSA included) with the maximum 64KB granule.
- A dense memory map, when the configuration parameter `DENSE_CS_ADDR_MAP` is 1. Each set of System registers is grouped on separate 4KB page boundaries. It may not be possible to isolate and remap individual components using an EL1 MMU with 16KB or 64KB granules. You can either use a 4KB granule, or depend on an EL2 MPU (or an EL1 MPU, if EL1 is using PMSA) to isolate components without remapping.

The following table shows the total space occupied by the Debug APB bus memory map, depending on how many cores are implemented in the processor.

**Table B-245: Debug APB bus sparse and dense memory map sizes**

Number of cores	Sparse memory map	Dense memory map
1	24-bit (16MB)	16-bit (64KB)
2	24-bit (16MB)	17-bit (128KB)
3	24-bit (16MB)	17-bit (128KB)
4	24-bit (16MB)	17-bit (128KB)
5	24-bit (16MB)	18-bit (256KB)
6	24-bit (16MB)	18-bit (256KB)
7	24-bit (16MB)	18-bit (256KB)

Number of cores	Sparse memory map	Dense memory map
8	24-bit (16MB)	18-bit (256KB)

The following table shows the base addresses for each set of system component registers that the external agents can access using the Debug APB bus.



The Debug APB memory map for the Cortex®-R82AE processor depends on the specific implementation of your cluster, for example the number of cores configured in the cluster or if the *Embedded Logic Analyzer* (ELA) included or not.

**Table B-246: Memory map for external agents accessing the Debug APB bus**

Base address, sparse map (DENSE_CS_ADDR_MAP = 0)	Base address, dense map (DENSE_CS_ADDR_MAP = 1)	Registers	Memory map
0x000000	0x00000	DebugBlock ROM Table	<a href="#">B.2.1.3 External DBROM registers summary on page 1712</a>
0x100000	0x0A000	Core 0 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x110000	0x10000	Core 1 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x120000	0x16000	Core 2 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x130000	0x1C000	Core 3 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x140000	0x22000	Core 4 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x150000	0x28000	Core 5 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x160000	0x2E000	Core 6 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x170000	0x34000	Core 7 CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x200000	0x01000	Cluster ROM Table	<a href="#">B.2.1.4 External CLUSTERROM registers summary on page 1713</a>
0x210000	0x02000	Cluster PMU	<a href="#">B.2.1.2 External CLUSTERPMU registers summary on page 1710</a>
0x220000	0x03000	Cluster ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0x230000	0x04000	Cluster CTI	<a href="#">B.2.1.6 External CTI registers summary on page 1716</a>
0x800000	0x05000	Core 0 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0x810000	0x06000	Core 0 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0x820000	0x07000	Core 0 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>

Base address, sparse map (DENSE_CS_ADDR_MAP = 0)	Base address, dense map (DENSE_CS_ADDR_MAP = 1)	Registers	Memory map
0x830000	0x08000	Core 0 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0x840000	0x09000	Core 0 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0x900000	0x0B000	Core 1 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0x910000	0x0C000	Core1 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0x920000	0x0D000	Core 1 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0x930000	0x0E000	Core 1 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0x940000	0x0F000	Core 1 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xA00000	0x11000	Core 2 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0xA10000	0x12000	Core 2 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xA20000	0x13000	Core 2 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xA30000	0x14000	Core 2 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xA40000	0x15000	Core 2 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xB00000	0x17000	Core 3 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0xB10000	0x18000	Core 3 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xB20000	0x19000	Core 3 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xB30000	0x1A000	Core 3 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xB40000	0x1B000	Core 3 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xC00000	0x1D000	Core 4 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0xC10000	0x1E000	Core 4 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xC20000	0x1F000	Core 4 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xC30000	0x20000	Core4 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xC40000	0x21000	Core 4 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xD00000	0x23000	Core 5 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>

Base address, sparse map (DENSE_CS_ADDR_MAP = 0)	Base address, dense map (DENSE_CS_ADDR_MAP = 1)	Registers	Memory map
0xD10000	0x24000	Core 5 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xD20000	0x25000	Core5 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xD30000	0x26000	Core5 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xD40000	0x27000	Core5 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xE00000	0x29000	Core 6 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0xE10000	0x2A000	Core 6 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xE20000	0x2B000	Core 6 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xE30000	0x2C000	Core 6 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xE40000	0x2D000	Core6 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>
0xF00000	0x2F000	Core 7 ROM Table	<a href="#">B.2.1.5 External COREROM registers summary on page 1715</a>
0xF10000	0x30000	Core 7 Debug	<a href="#">B.2.1.1 External Debug registers summary on page 1708</a>
0xF20000	0x31000	Core 7 PMU	<a href="#">B.2.1.8 External PMU registers summary on page 1721</a>
0xF30000	0x32000	Core 7 ETM	<a href="#">B.2.1.7 External ETM registers summary on page 1717</a>
0xF40000	0x33000	Core 7 ELA	See <a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>

## B.2.1 Register summaries for registers accessed over the Debug APB bus

This section includes the summary tables for all the external registers in the Cortex®-R82AE processor accessed over the Debug APB bus.

### B.2.1.1 External Debug registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped Debug registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).



**Table B-247: Debug registers summary**

Offset	Name	Reset	Width	Description
0x020	EDESR	See individual bit resets.	32-bit	External Debug Event Status Register
0x024	EDECR	See individual bit resets.	32-bit	External Debug Execution Control Register
0x030	EDWAR	See individual bit resets.	64-bit	External Debug Watchpoint Address Register
0x080	DBGDTRRX_ELO	See individual bit resets.	32-bit	Debug Data Transfer Register, Receive
0x084	EDITR	See individual bit resets.	32-bit	External Debug Instruction Transfer Register
0x088	EDSCR	See individual bit resets.	32-bit	External Debug Status and Control Register
0x08C	DBGDTRTX_ELO	See individual bit resets.	32-bit	Debug Data Transfer Register, Transmit
0x090	EDRCR	See individual bit resets.	32-bit	External Debug Reserve Control Register
0x098	EDECCR	See individual bit resets.	32-bit	External Debug Exception Catch Control Register
0x300	OSLAR_EL1	See individual bit resets.	32-bit	OS Lock Access Register
0x310	EDPRCR	See individual bit resets.	32-bit	External Debug Power/Reset Control Register
0x314	EDPRSR	See individual bit resets.	32-bit	External Debug Processor Status Register
0x400 + (16 * n)	DBGBVR<n>_EL1 [63:0]	See individual bit resets.	64-bit	Debug Breakpoint Value Registers
0x408 + (16 * n)	DBGBCR<n>_EL1	See individual bit resets.	64-bit	Debug Breakpoint Control Registers
0x800 + (16 * n)	DBGWVR<n>_EL1 [63:0]	See individual bit resets.	64-bit	Debug Watchpoint Value Registers
0x808 + (16 * n)	DBGWCR<n>_EL1	See individual bit resets.	64-bit	Debug Watchpoint Control Registers
0xD00	MIDR_EL1	See individual bit resets.	32-bit	Main ID Register
0xD20	EDPFR [31:0]	See individual bit resets.	32-bit	External Debug Processor Feature Register
0xD24	EDPFR [63:32]	See individual bit resets.	32-bit	External Debug Processor Feature Register
0xD28	EDDFR [31:0]	See individual bit resets.	32-bit	External Debug Feature Register
0xD2C	EDDFR [63:32]	See individual bit resets.	32-bit	External Debug Feature Register
0xD60	EDAA32PFR	See individual bit resets.	64-bit	External Debug Auxiliary Processor Feature Register
0xF00	EDITCTRL	See individual bit resets.	32-bit	External Debug Integration mode Control register
0xFA0	DBGCLAIMSET_EL1	See individual bit resets.	32-bit	Debug CLAIM Tag Set Register
0xFA4	DBGCLAIMCLR_EL1	See individual bit resets.	32-bit	Debug CLAIM Tag Clear Register
0xFA8	EDDEVAFF0	See individual bit resets.	32-bit	External Debug Device Affinity register 0
0xFAC	EDDEVAFF1	See individual bit resets.	32-bit	External Debug Device Affinity register 1
0xFB0	EDLAR	See individual bit resets.	32-bit	External Debug Lock Access Register
0xFB4	EDLSR	See individual bit resets.	32-bit	External Debug Lock Status Register
0xFB8	DBGAUTHSTATUS_EL1	See individual bit resets.	32-bit	Debug Authentication Status Register
0xFBC	EDDEVARCH	See individual bit resets.	32-bit	External Debug Device Architecture Register
0xFC0	EDDEVID2	See individual bit resets.	32-bit	External Debug Device ID register 2
0xFC4	EDDEVID1	See individual bit resets.	32-bit	External Debug Device ID Register 1
0xFC8	EDDEVID	See individual bit resets.	32-bit	External Debug Device ID register 0
0xFCC	EDDEVTYPE	See individual bit resets.	32-bit	External Debug Device Type register
0xFD0	EDPIDR4	See individual bit resets.	32-bit	External Debug Peripheral Identification Register 4
0xFE0	EDPIDR0	See individual bit resets.	32-bit	External Debug Peripheral Identification Register 0
0xFE4	EDPIDR1	See individual bit resets.	32-bit	External Debug Peripheral Identification Register 1
0xFE8	EDPIDR2	See individual bit resets.	32-bit	External Debug Peripheral Identification Register 2

Offset	Name	Reset	Width	Description
0xFEC	EDPIDR3	See individual bit resets.	32-bit	External Debug Peripheral Identification Register 3
0xFF0	EDCIDR0	See individual bit resets.	32-bit	External Debug Component Identification Register 0
0xFF4	EDCIDR1	See individual bit resets.	32-bit	External Debug Component Identification Register 1
0xFF8	EDCIDR2	See individual bit resets.	32-bit	External Debug Component Identification Register 2
0xFFC	EDCIDR3	See individual bit resets.	32-bit	External Debug Component Identification Register 3

### B.2.1.2 External CLUSTERPMU registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped CLUSTERPMU registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-248: CLUSTERPMU registers summary**

Offset	Name	Reset	Width	Description
0x000 + (8 * n)	<a href="#">CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Event Count Registers
0x0F8	<a href="#">CLUSTERPMU_PMCCNTR_EL1 [31:0]</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Cycle Counter
0x0FC	<a href="#">CLUSTERPMU_PMCCNTR_EL1 [63:32]</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Cycle Counter
0x400 + (4 * n)	<a href="#">CLUSTERPMU_PMEVTYPER&lt;n&gt;_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Event Type Registers
0x47C	<a href="#">CLUSTERPMU_PMCCFILTR_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Cycle Counter Filter Register
0xC00	<a href="#">CLUSTERPMU_PMCNTENSET_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Count Enable Set register
0xC20	<a href="#">CLUSTERPMU_PMCNTENCLR_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Count Enable Clear register
0xC40	<a href="#">CLUSTERPMU_PMINTENSET_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Interrupt Enable Set register
0xC60	<a href="#">CLUSTERPMU_PMINTENCLR_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Interrupt Enable Clear register
0xC80	<a href="#">CLUSTERPMU_PMOVSLR_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Overflow Flag Status Clear register
0xCA0	<a href="#">CLUSTERPMU_PMSWINC_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Software Increment register
0xCC0	<a href="#">CLUSTERPMU_PMOVSSSET_EL1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Overflow Flag Status Set register
0xE00	<a href="#">CLUSTERPMU_PMCFGR</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Configuration Register

Offset	Name	Reset	Width	Description
0xE04	CLUSTERPMU_PMCR_EL1	See individual bit resets.	32-bit	Cluster Performance Monitors Control Register
0xE20	CLUSTERPMU_PMCEID0	See individual bit resets.	32-bit	Cluster Performance Monitors Common Event Identification register 0
0xE24	CLUSTERPMU_PMCEID1	See individual bit resets.	32-bit	Cluster Performance Monitors Common Event Identification register 1
0xE28	CLUSTERPMU_PMCEID2	See individual bit resets.	32-bit	Cluster Performance Monitors Common Event Identification register 2
0xE2C	CLUSTERPMU_PMCEID3	See individual bit resets.	32-bit	Cluster Performance Monitors Common Event Identification register 3
0xE40	CLUSTERPMU_PMMIR	See individual bit resets.	32-bit	Cluster Performance Monitors Machine Identification Register
0xF00	CLUSTERPMU_PMITCTRL	See individual bit resets.	32-bit	Cluster Performance Monitors Integration mode Control register
0xFA0	CLUSTERPMU_PMCLAIMSET_EL1	See individual bit resets.	32-bit	Cluster Performance Monitors Claim Set register
0xFA4	CLUSTERPMU_PMCLAIMCLR_EL1	See individual bit resets.	32-bit	Cluster Performance Monitors Claim Clear register
0xFA8	CLUSTERPMU_PMDEVAFF0	See individual bit resets.	32-bit	Cluster Performance Monitors Device Affinity register 0
0xFAC	CLUSTERPMU_PMDEVAFF1	See individual bit resets.	32-bit	Cluster Performance Monitors Device Affinity register 1
0xFB0	CLUSTERPMU_PMLAR	See individual bit resets.	32-bit	Cluster Performance Monitors Lock Access Register
0xFB4	CLUSTERPMU_PMLSR	See individual bit resets.	32-bit	Cluster Performance Monitors Lock Status Register
0xFB8	CLUSTERPMU_PMAUTHSTATUS	See individual bit resets.	32-bit	Cluster Performance Monitors Authentication Status register
0xFBC	CLUSTERPMU_PMDEVARCH	See individual bit resets.	32-bit	Cluster Performance Monitors Device Architecture register
0xFC8	CLUSTERPMU_PMDEVID	See individual bit resets.	32-bit	Cluster Performance Monitors Device ID register
0xFCC	CLUSTERPMU_PMDEVTYPE	See individual bit resets.	32-bit	Cluster Performance Monitors Device Type register
0xFD0	CLUSTERPMU_PMPIDR4	See individual bit resets.	32-bit	Cluster Performance Monitors Peripheral Identification Register 4
0xFE0	CLUSTERPMU_PMPIDR0	See individual bit resets.	32-bit	Cluster Performance Monitors Peripheral Identification Register 0
0xFE4	CLUSTERPMU_PMPIDR1	See individual bit resets.	32-bit	Cluster Performance Monitors Peripheral Identification Register 1
0xFE8	CLUSTERPMU_PMPIDR2	See individual bit resets.	32-bit	Cluster Performance Monitors Peripheral Identification Register 2
0xFEC	CLUSTERPMU_PMPIDR3	See individual bit resets.	32-bit	Cluster Performance Monitors Peripheral Identification Register 3
0xFF0	CLUSTERPMU_PMCIDR0	See individual bit resets.	32-bit	Cluster Performance Monitors Component Identification Register 0

Offset	Name	Reset	Width	Description
0xFF4	<a href="#">CLUSTERPMU_PMCIDR1</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Component Identification Register 1
0xFF8	<a href="#">CLUSTERPMU_PMCIDR2</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Component Identification Register 2
0xFFC	<a href="#">CLUSTERPMU_PMCIDR3</a>	See individual bit resets.	32-bit	Cluster Performance Monitors Component Identification Register 3

### B.2.1.3 External DBROM registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped DBROM registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-249: DBROM registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">DBROM_ROMENTRY0</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 0
0x004	<a href="#">DBROM_ROMENTRY1</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 1
0x008	<a href="#">DBROM_ROMENTRY2</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 2
0x00C	<a href="#">DBROM_ROMENTRY3</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 3
0x010	<a href="#">DBROM_ROMENTRY4</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 4
0x014	<a href="#">DBROM_ROMENTRY5</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 5
0x018	<a href="#">DBROM_ROMENTRY6</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 6
0x01C	<a href="#">DBROM_ROMENTRY7</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 7
0x020	<a href="#">DBROM_ROMENTRY8</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 8
0x024	<a href="#">DBROM_ROMENTRY9</a>	See individual bit resets.	32-bit	DebugBlock ROM table Entry 9
0xA00	<a href="#">DBROM_DBGPCRO</a>	See individual bit resets.	32-bit	DebugBlock ROM table Debug Power Control Register 0
0xA80	<a href="#">DBROM_DBGPSRO</a>	See individual bit resets.	32-bit	DebugBlock ROM table Debug Power Status Register 0
0xC00	<a href="#">DBROM_PRIDRO</a>	See individual bit resets.	32-bit	DebugBlock ROM table Power Request ID Register 0
0xF00	<a href="#">DBROM_ITCTRL</a>	See individual bit resets.	32-bit	DebugBlock ROM table Integration Mode Control Register
0xFA0	<a href="#">DBROM_CLAIMSET</a>	See individual bit resets.	32-bit	DebugBlock ROM table Claim Tag Set Register
0xFA4	<a href="#">DBROM_CLAIMCLR</a>	See individual bit resets.	32-bit	DebugBlock ROM table Claim Tag Clear Register
0xFA8	<a href="#">DBROM_DEVAFF0</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Affinity Register 0
0xFAC	<a href="#">DBROM_DEVAFF1</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Affinity Register 1
0xFB0	<a href="#">DBROM_LAR</a>	See individual bit resets.	32-bit	DebugBlock ROM table Software Lock Access Register
0xFB4	<a href="#">DBROM_LSR</a>	See individual bit resets.	32-bit	DebugBlock ROM table Software Lock Status Register
0xFB8	<a href="#">DBROM_AUTHSTATUS</a>	See individual bit resets.	32-bit	DebugBlock ROM table Authentication Status Register
0xFBC	<a href="#">DBROM_DEVARCH</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Architecture Register

Offset	Name	Reset	Width	Description
0xFC0	<a href="#">DBROM_DEVID2</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Configuration Register 2
0xFC4	<a href="#">DBROM_DEVID1</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Configuration Register 1
0xFC8	<a href="#">DBROM_DEVID</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Configuration Register
0xFCC	<a href="#">DBROM_DEVTYPE</a>	See individual bit resets.	32-bit	DebugBlock ROM table Device Type Register
0xFD0	<a href="#">DBROM_PIDR4</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 4
0xFD4	<a href="#">DBROM_PIDR5</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 5
0xFD8	<a href="#">DBROM_PIDR6</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 6
0xFDC	<a href="#">DBROM_PIDR7</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 7
0xFE0	<a href="#">DBROM_PIDR0</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 0
0xFE4	<a href="#">DBROM_PIDR1</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 1
0xFE8	<a href="#">DBROM_PIDR2</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 2
0xFEC	<a href="#">DBROM_PIDR3</a>	See individual bit resets.	32-bit	DebugBlock ROM table Peripheral Identification Register 3
0xFF0	<a href="#">DBROM_CIDR0</a>	See individual bit resets.	32-bit	DebugBlock ROM table Component Identification Register 0
0xFF4	<a href="#">DBROM_CIDR1</a>	See individual bit resets.	32-bit	DebugBlock ROM table Component Identification Register 1
0xFF8	<a href="#">DBROM_CIDR2</a>	See individual bit resets.	32-bit	DebugBlock ROM table Component Identification Register 2
0xFFC	<a href="#">DBROM_CIDR3</a>	See individual bit resets.	32-bit	DebugBlock ROM table Component Identification Register 3

#### B.2.1.4 External CLUSTERROM registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped CLUSTERROM registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-250: CLUSTERROM registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">CLUSTERROM_ROMENTRY0</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 0
0x004	<a href="#">CLUSTERROM_ROMENTRY1</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 1
0x008	<a href="#">CLUSTERROM_ROMENTRY2</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 2
0x00C	<a href="#">CLUSTERROM_ROMENTRY3</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 3
0x010	<a href="#">CLUSTERROM_ROMENTRY4</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 4
0x014	<a href="#">CLUSTERROM_ROMENTRY5</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 5
0x018	<a href="#">CLUSTERROM_ROMENTRY6</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 6
0x01C	<a href="#">CLUSTERROM_ROMENTRY7</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 7
0x020	<a href="#">CLUSTERROM_ROMENTRY8</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 8
0x024	<a href="#">CLUSTERROM_ROMENTRY9</a>	See individual bit resets.	32-bit	Cluster ROM table Entry 9
0xA00	<a href="#">CLUSTERROM_DBGPCRO</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 0

Offset	Name	Reset	Width	Description
0xA04	<a href="#">CLUSTERROM_DBGPCR1</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 1
0xA08	<a href="#">CLUSTERROM_DBGPCR2</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 2
0xA0C	<a href="#">CLUSTERROM_DBGPCR3</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 3
0xA10	<a href="#">CLUSTERROM_DBGPCR4</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 4
0xA14	<a href="#">CLUSTERROM_DBGPCR5</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 5
0xA18	<a href="#">CLUSTERROM_DBGPCR6</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 6
0xA1C	<a href="#">CLUSTERROM_DBGPCR7</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Control Register 7
0xA80	<a href="#">CLUSTERROM_DBGPSR0</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 0
0xA84	<a href="#">CLUSTERROM_DBGPSR1</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 1
0xA88	<a href="#">CLUSTERROM_DBGPSR2</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 2
0xA8C	<a href="#">CLUSTERROM_DBGPSR3</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 3
0xA90	<a href="#">CLUSTERROM_DBGPSR4</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 4
0xA94	<a href="#">CLUSTERROM_DBGPSR5</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 5
0xA98	<a href="#">CLUSTERROM_DBGPSR6</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 6
0xA9C	<a href="#">CLUSTERROM_DBGPSR7</a>	See individual bit resets.	32-bit	Cluster ROM table Debug Power Status Register 7
0xC00	<a href="#">CLUSTERROM_PRIDR0</a>	See individual bit resets.	32-bit	Cluster ROM table Power Request ID Register 0
0xF00	<a href="#">CLUSTERROM_ITCTRL</a>	See individual bit resets.	32-bit	Cluster ROM table Integration Mode Control Register
0xFA0	<a href="#">CLUSTERROM_CLAIMSET</a>	See individual bit resets.	32-bit	Cluster ROM table Claim Tag Set Register
0xFA4	<a href="#">CLUSTERROM_CLAIMCLR</a>	See individual bit resets.	32-bit	Cluster ROM table Claim Tag Clear Register
0xFA8	<a href="#">CLUSTERROM_DEVAFF0</a>	See individual bit resets.	32-bit	Cluster ROM table Device Affinity Register 0
0xFAC	<a href="#">CLUSTERROM_DEVAFF1</a>	See individual bit resets.	32-bit	Cluster ROM table Device Affinity Register 1
0xFB0	<a href="#">CLUSTERROM_LAR</a>	See individual bit resets.	32-bit	Cluster ROM table Software Lock Access Register
0xFB4	<a href="#">CLUSTERROM_LSR</a>	See individual bit resets.	32-bit	Cluster ROM table Software Lock Status Register
0xFB8	<a href="#">CLUSTERROM_AUTHSTATUS</a>	See individual bit resets.	32-bit	Cluster ROM table Authentication Status Register
0xFBC	<a href="#">CLUSTERROM_DEVARCH</a>	See individual bit resets.	32-bit	Cluster ROM table Device Architecture Register
0xFC0	<a href="#">CLUSTERROM_DEVID2</a>	See individual bit resets.	32-bit	Cluster ROM table Device Configuration Register 2
0xFC4	<a href="#">CLUSTERROM_DEVID1</a>	See individual bit resets.	32-bit	Cluster ROM table Device Configuration Register 1
0xFC8	<a href="#">CLUSTERROM_DEVID</a>	See individual bit resets.	32-bit	Cluster ROM table Device Configuration Register
0xFCC	<a href="#">CLUSTERROM_DEVTYPE</a>	See individual bit resets.	32-bit	Cluster ROM table Device Type Register
0xFD0	<a href="#">CLUSTERROM_PIDR4</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 4
0xFD4	<a href="#">CLUSTERROM_PIDR5</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 5
0xFD8	<a href="#">CLUSTERROM_PIDR6</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 6
0xFDC	<a href="#">CLUSTERROM_PIDR7</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 7
0xFE0	<a href="#">CLUSTERROM_PIDR0</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 0
0xFE4	<a href="#">CLUSTERROM_PIDR1</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 1
0xFE8	<a href="#">CLUSTERROM_PIDR2</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 2
0xFEC	<a href="#">CLUSTERROM_PIDR3</a>	See individual bit resets.	32-bit	Cluster ROM table Peripheral Identification Register 3
0xFF0	<a href="#">CLUSTERROM_CIDR0</a>	See individual bit resets.	32-bit	Cluster ROM table Component Identification Register 0
0xFF4	<a href="#">CLUSTERROM_CIDR1</a>	See individual bit resets.	32-bit	Cluster ROM table Component Identification Register 1
0xFF8	<a href="#">CLUSTERROM_CIDR2</a>	See individual bit resets.	32-bit	Cluster ROM table Component Identification Register 2

Offset	Name	Reset	Width	Description
0xFFC	<a href="#">CLUSTERROM_CIDR3</a>	See individual bit resets.	32-bit	Cluster ROM table Component Identification Register 3

### B.2.1.5 External COREROM registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped COREROM registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-251: COREROM registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">COREROM_ROMENTRY0</a>	See individual bit resets.	32-bit	Core ROM table Entry 0
0x004	<a href="#">COREROM_ROMENTRY1</a>	See individual bit resets.	32-bit	Core ROM table Entry 1
0x008	<a href="#">COREROM_ROMENTRY2</a>	See individual bit resets.	32-bit	Core ROM table Entry 2
0x00C	<a href="#">COREROM_ROMENTRY3</a>	See individual bit resets.	32-bit	Core ROM table Entry 3
0xC00	<a href="#">COREROM_PRIDR0</a>	See individual bit resets.	32-bit	Core ROM table Power Request ID Register 0
0xF00	<a href="#">COREROM_ITCTRL</a>	See individual bit resets.	32-bit	Core ROM table Integration Mode Control Register
0xFA0	<a href="#">COREROM_CLAIMSET</a>	See individual bit resets.	32-bit	Core ROM table Claim Tag Set Register
0xFA4	<a href="#">COREROM_CLAIMCLR</a>	See individual bit resets.	32-bit	Core ROM table Claim Tag Clear Register
0xFA8	<a href="#">COREROM_DEVAFF0</a>	See individual bit resets.	32-bit	Core ROM table Device Affinity Register 0
0xFAC	<a href="#">COREROM_DEVAFF1</a>	See individual bit resets.	32-bit	Core ROM table Device Affinity Register 1
0xFB0	<a href="#">COREROM_LAR</a>	See individual bit resets.	32-bit	Core ROM table Software Lock Access Register
0xFB4	<a href="#">COREROM_LSR</a>	See individual bit resets.	32-bit	Core ROM table Software Lock Status Register
0xFB8	<a href="#">COREROM_AUTHSTATUS</a>	See individual bit resets.	32-bit	Core ROM table Authentication Status Register
0xFBC	<a href="#">COREROM_DEVARCH</a>	See individual bit resets.	32-bit	Core ROM table Device Architecture Register
0xFC0	<a href="#">COREROM_DEVID2</a>	See individual bit resets.	32-bit	Core ROM table Device Configuration Register 2
0xFC4	<a href="#">COREROM_DEVID1</a>	See individual bit resets.	32-bit	Core ROM table Device Configuration Register 1
0xFC8	<a href="#">COREROM_DEVID</a>	See individual bit resets.	32-bit	Core ROM table Device Configuration Register
0xFCC	<a href="#">COREROM_DEVTYPE</a>	See individual bit resets.	32-bit	Core ROM table Device Type Register
0xFD0	<a href="#">COREROM_PIDR4</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 4
0xFD4	<a href="#">COREROM_PIDR5</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 5
0xFD8	<a href="#">COREROM_PIDR6</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 6
0xFDC	<a href="#">COREROM_PIDR7</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 7
0xFE0	<a href="#">COREROM_PIDR0</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 0
0xFE4	<a href="#">COREROM_PIDR1</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 1
0xFE8	<a href="#">COREROM_PIDR2</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 2
0xFEC	<a href="#">COREROM_PIDR3</a>	See individual bit resets.	32-bit	Core ROM table Peripheral Identification Register 3



Offset	Name	Reset	Width	Description
0xFF0	<a href="#">COREROM_CIDR0</a>	See individual bit resets.	32-bit	Core ROM table Component Identification Register 0
0xFF4	<a href="#">COREROM_CIDR1</a>	See individual bit resets.	32-bit	Core ROM table Component Identification Register 1
0xFF8	<a href="#">COREROM_CIDR2</a>	See individual bit resets.	32-bit	Core ROM table Component Identification Register 2
0xFFC	<a href="#">COREROM_CIDR3</a>	See individual bit resets.	32-bit	Core ROM table Component Identification Register 3

### B.2.1.6 External CTI registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped CTI registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-252: CTI registers summary**

Offset	Name	Reset	Width	Description
0x000	<a href="#">CTICONTROL</a>	See individual bit resets.	32-bit	CTI Control register
0x010	<a href="#">CTIINTACK</a>	See individual bit resets.	32-bit	CTI Output Trigger Acknowledge register
0x014	<a href="#">CTIAPPSET</a>	See individual bit resets.	32-bit	CTI Application Trigger Set register
0x018	<a href="#">CTIAPPCLEAR</a>	See individual bit resets.	32-bit	CTI Application Trigger Clear register
0x01C	<a href="#">CTIAPPPULSE</a>	See individual bit resets.	32-bit	CTI Application Pulse register
0x020 + (4 * n)	<a href="#">CTIINEN&lt;n&gt;</a>	See individual bit resets.	32-bit	CTI Input Trigger to Output Channel Enable registers
0x0A0 + (4 * n)	<a href="#">CTIOUTEN&lt;n&gt;</a>	See individual bit resets.	32-bit	CTI Input Channel to Output Trigger Enable registers
0x130	<a href="#">CTITRIGINSTATUS</a>	See individual bit resets.	32-bit	CTI Trigger In Status register
0x134	<a href="#">CTITRIGOUTSTATUS</a>	See individual bit resets.	32-bit	CTI Trigger Out Status register
0x138	<a href="#">CTICHINSTATUS</a>	See individual bit resets.	32-bit	CTI Channel In Status register
0x13C	<a href="#">CTICHOUTSTATUS</a>	See individual bit resets.	32-bit	CTI Channel Out Status register
0x140	<a href="#">CTIGATE</a>	See individual bit resets.	32-bit	CTI Channel Gate Enable register
0x144	<a href="#">ASICCTL</a>	See individual bit resets.	32-bit	CTI External Multiplexer Control register
0x150	<a href="#">CTIDEVCTL</a>	See individual bit resets.	32-bit	CTI Device Control register
0xF00	<a href="#">CTIITCTRL</a>	See individual bit resets.	32-bit	CTI Integration mode Control register
0xFA0	<a href="#">CTICLAIMSET</a>	See individual bit resets.	32-bit	CTI Claim Tag Set register
0xFA4	<a href="#">CTICLAIMCLR</a>	See individual bit resets.	32-bit	CTI Claim Tag Clear register
0xFA8	<a href="#">CTIDEVAFF0</a>	See individual bit resets.	32-bit	CTI Device Affinity register 0
0xFAC	<a href="#">CTIDEVAFF1</a>	See individual bit resets.	32-bit	CTI Device Affinity register 1
0xFB0	<a href="#">CTILAR</a>	See individual bit resets.	32-bit	CTI Lock Access Register
0xFB4	<a href="#">CTILSR</a>	See individual bit resets.	32-bit	CTI Lock Status Register
0xFB8	<a href="#">CTIAUTHSTATUS</a>	See individual bit resets.	32-bit	CTI Authentication Status register
0xFBC	<a href="#">CTIDEVARCH</a>	See individual bit resets.	32-bit	CTI Device Architecture register



Offset	Name	Reset	Width	Description
0xFC0	<a href="#">CTIDEVID2</a>	See individual bit resets.	32-bit	CTI Device ID register 2
0xFC4	<a href="#">CTIDEVID1</a>	See individual bit resets.	32-bit	CTI Device ID register 1
0xFC8	<a href="#">CTIDEVID</a>	See individual bit resets.	32-bit	CTI Device ID register 0
0xFCC	<a href="#">CTIDEVTYPE</a>	See individual bit resets.	32-bit	CTI Device Type register
0xFD0	<a href="#">CTIPIDR4</a>	See individual bit resets.	32-bit	CTI Peripheral Identification Register 4
0xFE0	<a href="#">CTIPIDR0</a>	See individual bit resets.	32-bit	CTI Peripheral Identification Register 0
0xFE4	<a href="#">CTIPIDR1</a>	See individual bit resets.	32-bit	CTI Peripheral Identification Register 1
0xFE8	<a href="#">CTIPIDR2</a>	See individual bit resets.	32-bit	CTI Peripheral Identification Register 2
0xFEC	<a href="#">CTIPIDR3</a>	See individual bit resets.	32-bit	CTI Peripheral Identification Register 3
0xFF0	<a href="#">CTICIDR0</a>	See individual bit resets.	32-bit	CTI Component Identification Register 0
0xFF4	<a href="#">CTICIDR1</a>	See individual bit resets.	32-bit	CTI Component Identification Register 1
0xFF8	<a href="#">CTICIDR2</a>	See individual bit resets.	32-bit	CTI Component Identification Register 2
0xFFC	<a href="#">CTICIDR3</a>	See individual bit resets.	32-bit	CTI Component Identification Register 3

### B.2.1.7 External ETM registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped ETM registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-253: ETM registers summary**

Offset	Name	Reset	Width	Description
0x004	<a href="#">TRCPRGCTLR</a>	See individual bit resets.	32-bit	Programming Control Register
0x00C	<a href="#">TRCSTATR</a>	See individual bit resets.	32-bit	Trace Status Register
0x010	<a href="#">TRCCONFIGR</a>	See individual bit resets.	32-bit	Trace Configuration Register
0x018	<a href="#">TRCAUXCTLR</a>	See individual bit resets.	32-bit	Auxillary Control Register
0x020	<a href="#">TRCEVENTCTLOR</a>	See individual bit resets.	32-bit	Event Control 0 Register
0x024	<a href="#">TRCEVENTCTL1R</a>	See individual bit resets.	32-bit	Event Control 1 Register
0x02C	<a href="#">TRCSTALLCTLR</a>	See individual bit resets.	32-bit	Stall Control Register
0x030	<a href="#">TRCTSCTLR</a>	See individual bit resets.	32-bit	Timestamp Control Register

Offset	Name	Reset	Width	Description
0x034	TRCSYNCPR	See individual bit resets.	32-bit	Synchronization Period Register
0x038	TRCCCCTLR	See individual bit resets.	32-bit	Cycle Count Control Register
0x03C	TRCBBCTLR	See individual bit resets.	32-bit	Branch Broadcast Control Register
0x040	TRCTRACEIDR	See individual bit resets.	32-bit	Trace ID Register
0x080	TRCVICTLR	See individual bit resets.	32-bit	ViewInst Main Control Register
0x084	TRCVIIECTLR	See individual bit resets.	32-bit	ViewInst Include/Exclude Control Register
0x088	TRCVISSCTLR	See individual bit resets.	32-bit	ViewInst Start/Stop Control Register
0x0A0	TRCVDCTLR	See individual bit resets.	32-bit	ViewData Main Control Register
0x0A4	TRCVDSACCTLR	See individual bit resets.	32-bit	ViewData Include/Exclude Single Address Comparator Control Register
0x0A8	TRCVDARCCTLR	See individual bit resets.	32-bit	ViewData Include/Exclude Address Range Comparator Control Register
0x100 + (4 * n)	TRCSEQEVR<n>	See individual bit resets.	32-bit	Sequencer State Transition Control Register <n>
0x118	TRCSEQRSTEVPR	See individual bit resets.	32-bit	Sequencer Reset Control Register
0x11C	TRCSEQSTR	See individual bit resets.	32-bit	Sequencer State Register
0x120	TRCEXTINSELPR	See individual bit resets.	32-bit	External Input Select Register
0x140 + (4 * n)	TRCCNTRLDVR<n>	See individual bit resets.	32-bit	Counter Reload Value Register <n>
0x150 + (4 * n)	TRCCNTCTLR<n>	See individual bit resets.	32-bit	Counter Control Register <n>
0x160 + (4 * n)	TRCCNTVR<n>	See individual bit resets.	32-bit	Counter Value Register <n>
0x180	TRCIDR8	See individual bit resets.	32-bit	ID Register 8
0x184	TRCIDR9	See individual bit resets.	32-bit	ID Register 9
0x188	TRCIDR10	See individual bit resets.	32-bit	ID Register 10
0x18C	TRCIDR11	See individual bit resets.	32-bit	ID Register 11
0x190	TRCIDR12	See individual bit resets.	32-bit	ID Register 12
0x194	TRCIDR13	See individual bit resets.	32-bit	ID Register 13

Offset	Name	Reset	Width	Description
0x1C0	TRCIMSPECO	See individual bit resets.	32-bit	IMP DEF Register 0
0x1E0	TRCIDR0	See individual bit resets.	32-bit	ID Register 0
0x1E4	TRCIDR1	See individual bit resets.	32-bit	ID Register 1
0x1E8	TRCIDR2	See individual bit resets.	32-bit	ID Register 2
0x1EC	TRCIDR3	See individual bit resets.	32-bit	ID Register 3
0x1F0	TRCIDR4	See individual bit resets.	32-bit	ID Register 4
0x1F4	TRCIDR5	See individual bit resets.	32-bit	ID Register 5
0x1F8	TRCIDR6	See individual bit resets.	32-bit	ID Register 6
0x1FC	TRCIDR7	See individual bit resets.	32-bit	ID Register 7
0x200 + (4 * n)	TRCRSCTLR<n>	See individual bit resets.	32-bit	Resource Selection Control Register <n>
0x280 + (4 * n)	TRCSSCCR<n>	See individual bit resets.	32-bit	Single-shot Comparator Control Register <n>
0x2A0 + (4 * n)	TRCSSCSR<n>	See individual bit resets.	32-bit	Single-shot Comparator Control Status Register <n>
0x300	TRCOSLAR	See individual bit resets.	32-bit	Trace OS Lock Access Register
0x304	TRCOSLSR	See individual bit resets.	32-bit	Trace OS Lock Status Register
0x310	TRCPDCR	See individual bit resets.	32-bit	PowerDown Control Register
0x314	TRCPDSR	See individual bit resets.	32-bit	PowerDown Status Register
0x400 + (8 * n)	TRCACVR<n>	See individual bit resets.	64-bit	Address Comparator Value Register <n>
0x480 + (8 * n)	TRCACATR<n>	See individual bit resets.	64-bit	Address Comparator Access Type Register <n>
0x500 + (16 * n)	TRCDVCVR<n>	See individual bit resets.	64-bit	Data Value Comparator Value Register <n>
0x580 + (16 * n)	TRCDVCMR<n>	See individual bit resets.	64-bit	Data Value Comparator Mask Register <n>
0x600 + (8 * n)	TRCCIDCVR<n>	See individual bit resets.	64-bit	Context Identifier Comparator Value Registers <n>
0x640 + (8 * n)	TRCVMIDCVR<n>	See individual bit resets.	64-bit	Virtual Context Identifier Comparator Value Register <n>
0x680	TRCCIDCCTLR0	See individual bit resets.	32-bit	Context Identifier Comparator Control Register 0

Offset	Name	Reset	Width	Description
0x688	TRCVMIDCCTRL0	See individual bit resets.	32-bit	Virtual Context Identifier Comparator Control Register 0
0xF00	TRCITCTRL	See individual bit resets.	32-bit	Integration Mode Control Register
0xFA0	TRCCLAIMSET	See individual bit resets.	32-bit	Claim Tag Set Register
0xFA4	TRCCLAIMCLR	See individual bit resets.	32-bit	Claim Tag Clear Register
0xFA8	TRCDEVAFF	See individual bit resets.	64-bit	Device Affinity Register
0xFB0	TRCLAR	See individual bit resets.	32-bit	Lock Access Register
0xFB4	TRCLSR	See individual bit resets.	32-bit	Lock Status Register
0xFB8	TRCAUTHSTATUS	See individual bit resets.	32-bit	Authentication Status Register
0xFBC	TRCDEVARCH	See individual bit resets.	32-bit	Device Architecture Register
0xFC8	TRCDEVID	See individual bit resets.	32-bit	Device Configuration Register
0xFCC	TRCDEVTYPE	See individual bit resets.	32-bit	Device Type Register
0xFD0	TRCPIDR4	See individual bit resets.	32-bit	Peripheral Identification Register 4
0xFD4	TRCPIDR5	See individual bit resets.	32-bit	Peripheral Identification Register 5
0xFD8	TRCPIDR6	See individual bit resets.	32-bit	Peripheral Identification Register 6
0xFDC	TRCPIDR7	See individual bit resets.	32-bit	Peripheral Identification Register 7
0xFE0	TRCPIDR0	See individual bit resets.	32-bit	Peripheral Identification Register 0
0xFE4	TRCPIDR1	See individual bit resets.	32-bit	Peripheral Identification Register 1
0xFE8	TRCPIDR2	See individual bit resets.	32-bit	Peripheral Identification Register 2
0xFEC	TRCPIDR3	See individual bit resets.	32-bit	Peripheral Identification Register 3
0xFF0	TRCCIDR0	See individual bit resets.	32-bit	Component Identification Register 0
0xFF4	TRCCIDR1	See individual bit resets.	32-bit	Component Identification Register 1
0xFF8	TRCCIDR2	See individual bit resets.	32-bit	Component Identification Register 2
0xFFC	TRCCIDR3	See individual bit resets.	32-bit	Component Identification Register 3

### B.2.1.8 External PMU registers summary

The following summary table provides an overview of **IMPLEMENTATION DEFINED** memory-mapped PMU registers in the core.

For more information on registers listed in the table, click on the link associated with the register name.

For registers without a listed reset value, refer to the individual field resets documented on the register description pages or to the [Arm® Architecture Reference Manual for A-profile architecture](#).

**Table B-254: PMU registers summary**

Offset	Name	Reset	Width	Description
0x000 + (8 * n)	<a href="#">PMEVCNTR&lt;n&gt;_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Event Count Registers
0x0F8	<a href="#">PMCCNTR_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Cycle Counter
0x0FC	<a href="#">PMCCNTR_ELO [63:32]</a>	See individual bit resets.	32-bit	Performance Monitors Cycle Counter
0x200	<a href="#">PMPCSR [31:0]</a>	See individual bit resets.	32-bit	Program Counter Sample Register
0x204	<a href="#">PMPCSR [63:32]</a>	See individual bit resets.	32-bit	Program Counter Sample Register
0x220	<a href="#">PMPCSR [31:0]</a>	See individual bit resets.	32-bit	Program Counter Sample Register
0x224	<a href="#">PMPCSR [63:32]</a>	See individual bit resets.	32-bit	Program Counter Sample Register
0x208	<a href="#">PMCID1SR</a>	See individual bit resets.	32-bit	CONTEXTIDR_EL1 Sample Register
0x228	<a href="#">PMCID1SR</a>	See individual bit resets.	32-bit	CONTEXTIDR_EL1 Sample Register
0x20C	<a href="#">PMVIDSR</a>	See individual bit resets.	32-bit	VMID Sample Register
0x22C	<a href="#">PMCID2SR</a>	See individual bit resets.	32-bit	CONTEXTIDR_EL2 Sample Register
0x400 + (4 * n)	<a href="#">PMEVTYPER&lt;n&gt;_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Event Type Registers
0x47C	<a href="#">PMCCFILTR_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Cycle Counter Filter Register
0xC00	<a href="#">PMCNTENSET_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Count Enable Set Register
0xC20	<a href="#">PMCNTENCLR_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Count Enable Clear Register
0xC40	<a href="#">PMINTENSET_EL1 [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Interrupt Enable Set Register
0xC60	<a href="#">PMINTENCLR_EL1 [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Interrupt Enable Clear Register

Offset	Name	Reset	Width	Description
0xC80	<a href="#">PMOVSLR_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Overflow Flag Status Clear register
0xCA0	<a href="#">PMSWINC_ELO</a>	See individual bit resets.	32-bit	Performance Monitors Software Increment Register
0xCC0	<a href="#">PMOVSSET_ELO [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Overflow Flag Status Set Register
0xE00	<a href="#">PMCFGR [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Configuration Register
0xE04	<a href="#">PMCR_ELO</a>	See individual bit resets.	32-bit	Performance Monitors Control Register
0xE20	<a href="#">PMCEID0</a>	See individual bit resets.	32-bit	Performance Monitors Common Event Identification register 0
0xE24	<a href="#">PMCEID1</a>	See individual bit resets.	32-bit	Performance Monitors Common Event Identification register 1
0xE28	<a href="#">PMCEID2</a>	See individual bit resets.	32-bit	Performance Monitors Common Event Identification register 2
0xE2C	<a href="#">PMCEID3</a>	See individual bit resets.	32-bit	Performance Monitors Common Event Identification register 3
0xE40	<a href="#">PMMIR [31:0]</a>	See individual bit resets.	32-bit	Performance Monitors Machine Identification Register
0xF00	<a href="#">PMITCTRL</a>	See individual bit resets.	32-bit	Performance Monitors Integration mode Control register
0xFA8	<a href="#">PMDEVAFF0</a>	See individual bit resets.	32-bit	Performance Monitors Device Affinity register 0
0xFAC	<a href="#">PMDEVAFF1</a>	See individual bit resets.	32-bit	Performance Monitors Device Affinity register 1
0xFB0	<a href="#">PMLAR</a>	See individual bit resets.	32-bit	Performance Monitors Lock Access Register
0xFB4	<a href="#">PMLSR</a>	See individual bit resets.	32-bit	Performance Monitors Lock Status Register
0xFB8	<a href="#">PMAUTHSTATUS</a>	See individual bit resets.	32-bit	Performance Monitors Authentication Status register
0xFBC	<a href="#">PMDEVARCH</a>	See individual bit resets.	32-bit	Performance Monitors Device Architecture register
0xFC8	<a href="#">PMDEVID</a>	See individual bit resets.	32-bit	Performance Monitors Device ID register
0xFCC	<a href="#">PMDEVTYPE</a>	See individual bit resets.	32-bit	Performance Monitors Device Type register
0xFD0	<a href="#">PMPIDR4</a>	See individual bit resets.	32-bit	Performance Monitors Peripheral Identification Register 4
0xFE0	<a href="#">PMPIDR0</a>	See individual bit resets.	32-bit	Performance Monitors Peripheral Identification Register 0
0xFE4	<a href="#">PMPIDR1</a>	See individual bit resets.	32-bit	Performance Monitors Peripheral Identification Register 1
0xFE8	<a href="#">PMPIDR2</a>	See individual bit resets.	32-bit	Performance Monitors Peripheral Identification Register 2

Offset	Name	Reset	Width	Description
0xFEC	PMPIDR3	See individual bit resets.	32-bit	Performance Monitors Peripheral Identification Register 3
0xFF0	PMCIDR0	See individual bit resets.	32-bit	Performance Monitors Component Identification Register 0
0xFF4	PMCIDR1	See individual bit resets.	32-bit	Performance Monitors Component Identification Register 1
0xFF8	PMCIDR2	See individual bit resets.	32-bit	Performance Monitors Component Identification Register 2
0xFFC	PMCIDR3	See individual bit resets.	32-bit	Performance Monitors Component Identification Register 3

## B.2.2 Register descriptions for registers accessed over the Debug APB bus

This section includes the descriptions for all the external registers in the Cortex®-R82AE processor accessed over the Debug APB bus.

### B.2.2.1 External Debug register description

This section includes the register descriptions for all memory-mapped Debug registers that are accessed for each core.

#### B.2.2.1.1 EDESR, External Debug Event Status Register

Indicates the status of internally pending Halting debug events.

#### Configurations

This register is available in all configurations.

#### Attributes

##### Width

32

##### Component

Debug

##### Register offset

0x020

##### Access type

RW1C

##### Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-123: EXT\_EDESR bit assignments

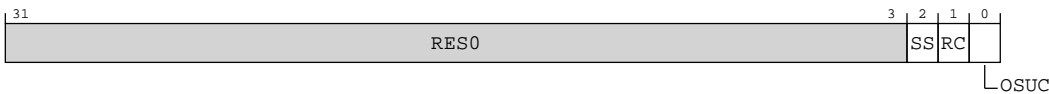


Table B-255: EDESR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	SS	Halting step debug event pending. Possible values of this field are:  <b>0b0</b> Reading this means that a Halting step debug event is not pending. Writing this means no action.  <b>0b1</b> Reading this means that a Halting step debug event is pending. Writing this clears the pending Halting step debug event.	0b0
[1]	RC	Reset Catch debug event pending. Possible values of this field are:  <b>0b0</b> Reading this means that a Reset Catch debug event is not pending. Writing this means no action.  <b>0b1</b> Reading this means that a Reset Catch debug event is pending. Writing this clears the pending Reset Catch debug event.	0b0
[0]	OSUC	OS Unlock Catch debug event pending. Possible values of this field are:  <b>0b0</b> Reading this means that an OS Unlock Catch debug event is not pending. Writing this means no action.  <b>0b1</b> Reading this means that an OS Unlock Catch debug event is pending. Writing this clears the pending OS Unlock Catch debug event.	0b0

Access

If a request to clear a pending Halting debug event is received at or about the time when halting becomes allowed, it is **CONSTRAINED UNPREDICTABLE** whether the event is taken.

If Core power is removed while a Halting debug event is pending, it is lost. However, it might become pending again when the Core is powered back on and Cold reset.

Accessibility

If a request to clear a pending Halting debug event is received at or about the time when halting becomes allowed, it is **CONSTRAINED UNPREDICTABLE** whether the event is taken.



If Core power is removed while a Halting debug event is pending, it is lost. However, it might become pending again when the Core is powered back on and Cold reset.

Component	Offset	Instance	Range
Debug	0x020	EDESR	None

This interface is accessible as follows:

When IsCorePowered()

RW

Otherwise

ERROR

B.2.2.1.2 EDECR, External Debug Execution Control Register

Controls Halting debug events.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0x024

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x0xx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-124: EXT\_EDECR bit assignments

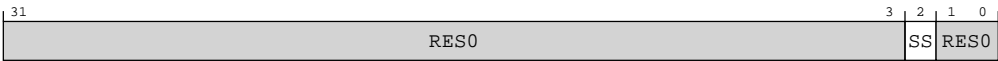


Table B-257: EDECR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	SS	Halting step enable. Possible values of this field are:  <b>0b0</b> Halting step debug event disabled.  <b>0b1</b> Halting step debug event enabled.  If the value of EDECR.SS is changed when the PE is in Non-debug state, behavior is CONSTRAINED UNPREDICTABLE. The implemented behavior is the value of ext-EDECR.SS becomes <b>UNKNOWN</b> .	0b0
[1:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
Debug	0x024	EDECR	None

This interface is accessible as follows:

When IsCorePowered()

RW

Otherwise

ERROR

B.2.2.1.3 EDWAR, External Debug Watchpoint Address Register

Returns the virtual data address being accessed when a Watchpoint Debug Event was triggered.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

Debug

Register offset

0x030

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-125: EXT\_EDWAR bit assignments

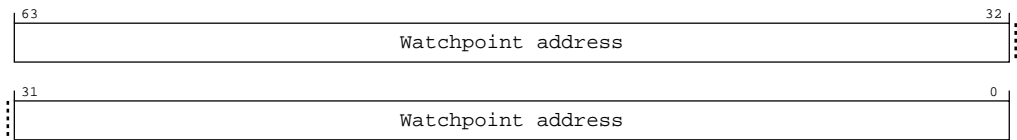


Table B-259: EDWAR bit descriptions

Bits	Name	Description	Reset
[63:0]	None	Watchpoint address. The data virtual address being accessed when a Watchpoint Debug Event was triggered and caused entry to Debug state. This address must be within a naturally-aligned block of memory of power-of-two size no larger than the DC ZVA block size.  The value of this register is <b>UNKNOWN</b> if the PE is in Non-debug state, or if Debug state was entered other than for a Watchpoint debug event.  The EDWAR is subject to the same alignment rules as the reporting of a watchpointed address in the FAR. See <i>Determining the memory location that caused a Watchpoint exception</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	64 {x}

Accessibility

Component	Offset	Instance	Range
Debug	0x030	EDWAR	None

This interface is accessible as follows:

When IsCorePowered() and !OSLockStatus()

RO

Otherwise

ERROR

B.2.2.1.4 DBGDTRRX\_EL0, Debug Data Transfer Register, Receive

Transfers data from an external debugger to the PE. For example, it is used by a debugger transferring commands and data to a debug target. See AArch64-DBGDTR\_EL0 for additional architectural mappings. It is a component of the Debug Communications Channel.

Configurations

External register DBGDTRRX\_EL0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.20 DBGDTRRX\\_EL0, Debug Data Transfer Register, Receive](#) on page 1116 bits [31:0].

Attributes

Width

32

Component

Debug

Register offset

0x080

Access type

See bit descriptions

Reset value

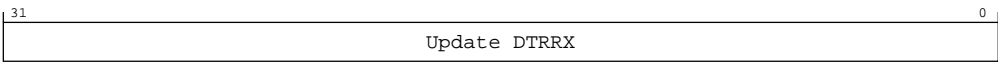
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-126: EXT\_DBGDTRRX\_EL0 bit assignments



**Table B-261: DBGDTRRX\_ELO bit descriptions**

Bits	Name	Description	Reset
[31:0]	None	<p>Update DTRRX.</p> <p>Writes to this register:</p> <ul style="list-style-type: none"> <li>If RXfull is set to 1, set DTRRX to <b>UNKNOWN</b>.</li> <li>If RXfull is set to 0, update the value in DTRRX.</li> </ul> <p>After the write, RXfull is set to 1.</p> <p>Reads of this register:</p> <ul style="list-style-type: none"> <li>If RXfull is set to 1, return the last value written to DTRRX.</li> <li>If RXfull is set to 0, return an <b>UNKNOWN</b> value.</li> </ul> <p>After the read, RXfull remains unchanged.</p> <p>For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	32 {x}

### Access

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any operation issued by a DTR access in memory access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.
- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an **UNKNOWN** state.

### Accessibility

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any operation issued by a DTR access in memory access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.
- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an **UNKNOWN** state.

Component	Offset	Instance	Range
Debug	0x080	DBGDTRRX_ELO	None

This interface is accessible as follows:

#### When IsCorePowered() and !OSLockStatus()

RW

#### Otherwise

ERROR

B.2.2.1.5     EDITR, External Debug Instruction Transfer Register

Used in Debug state for passing instructions to the PE for execution.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

Debug

Register offset

0x084

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-127: EXT\_EDITR bit assignments

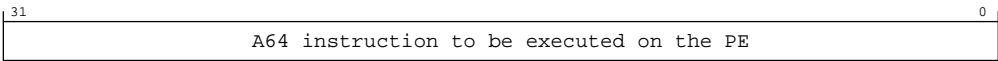


Table B-263: EDITR bit descriptions

Bits	Name	Description	Reset
[31:0]	None	A64 instruction to be executed on the PE.	32 {x}

Access

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any instruction issued through the ITR in Normal access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.

- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an **UNKNOWN** state.

EDITR ignores writes if the PE is in Non-debug state.

Accessibility

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any instruction issued through the ITR in Normal access mode that has not completed execution is CONSTRAINED UNPREDICTABLE, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.
- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an UNKNOWN state.

EDITR ignores writes if the PE is in Non-debug state.

Component	Offset	Instance	Range
Debug	0x084	EDITR	None

This interface is accessible as follows:

**When IsCorePowered() and !OSLockStatus()**  
    WO  
**Otherwise**  
    ERROR

B.2.2.1.6     EDSCR, External Debug Status and Control Register

Main control register for the debug implementation.

Configurations

External register EDSCR bits [30:29] are architecturally mapped to AArch64 System register [A.2.5.18 MDCCSR\\_ELO, Monitor DCC Status Register](#) on page 1112 bits [30:29].

Attributes

**Width**  
    32  
**Component**  
    Debug  
**Register offset**  
    0x088  
**Access type**  
    inconsistent

Reset value

000x	00xx	0000	xxxx	x011	11xx	x0xx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-128: EXT\_EDSCR bit assignments

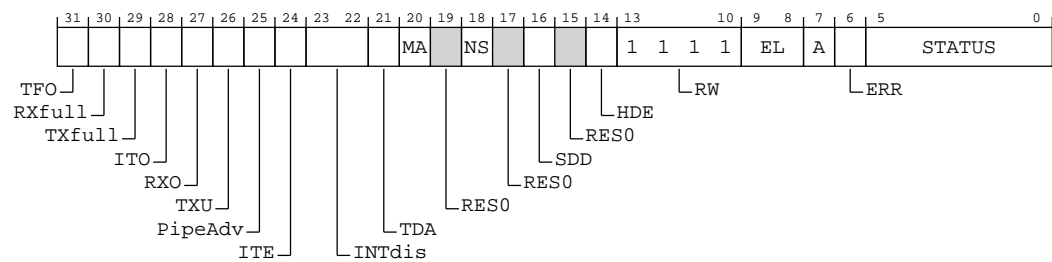


Table B-265: EDSCR bit descriptions

Bits	Name	Description	Reset
[31]	TFO	Trace Filter Override. Overrides the Trace Filter controls allowing the external debugger to trace any visible Exception level.  <b>0b0</b> Trace Filter controls are not affected.  <b>0b1</b> Trace Filter controls in AArch64-TRFCR_EL1 and AArch64-TRFCR_EL2 are ignored.  When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers: <ul style="list-style-type: none"><li>AArch64-MDSCR_EL1.</li></ul> This bit is ignored by the PE when ExternalSecureNoninvasiveDebugEnabled() is FALSE and the Effective value of AArch64-MDCR_EL3.STE is 1.	0b0
[30]	RXfull	DTRRX full.  When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers: <ul style="list-style-type: none"><li>AArch64-MDSCR_EL1.</li></ul> Access to this field is: RO	0b0



Bits	Name	Description	Reset
[29]	TXfull	DTRTX full.  When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers: <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul> Access to this field is: RO	0b0
[28]	ITO	ITR overrun. Set to 0 on entry to Debug state.  <b>When !Halted()</b> Access to this field is: <b>UNKNOWN/WI</b>  <b>Otherwise</b> Access to this field is: RO	x
[27]	RXO	DTRRX overrun.  When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers: <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul> Access to this field is: RO	0b0
[26]	TXU	DTRTX underrun.  When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers: <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul> Access to this field is: RO	0b0
[25]	PipeAdv	Pipeline Advance. Indicates that software execution is progressing.  <b>0b0</b> No progress has been made by the PE since the last time this field was cleared to zero by writing 1 to ext-EDRCR.CSPA.  <b>0b1</b> Progress has been made by the PE since the last time this field was cleared to zero by writing 1 to ext-EDRCR.CSPA.  The architecture does not define precisely when this field is set to 1. It requires only that this happen periodically in Non-debug state to indicate that software execution is progressing. For example, a PE might set this field to 1 each time the PE retires one or more instructions, or at periodic intervals during the progression of an instruction.  Access to this field is: RO	x
[24]	ITE	ITR empty.  <b>When !Halted()</b> Access to this field is: <b>UNKNOWN/WI</b>  <b>Otherwise</b> Access to this field is: RO	x

Bits	Name	Description	Reset
[23:22]	INTdis	<p>Interrupt disable. Disables taking interrupts in Non-debug state.</p> <p><b>0b00</b></p> <p>Masking of interrupts is controlled by PSTATE and interrupt routing controls.</p> <p><b>0b01</b></p> <p>If ExternalInvasiveDebugEnabled() is TRUE, then all interrupts taken to Non-secure state are masked.</p> <p>If ExternalSecureInvasiveDebugEnabled() is TRUE, then all interrupts taken to Secure state are masked.</p> <p><b>Note:</b></p> <p>All interrupts includes virtual and SError interrupts.</p> <p>When AArch64-OSLSR_EL1.OSLK is 1, this field can be indirectly read and written through the following System registers:</p> <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul> <p>The Effective value of this field is 0b00 when ExternalInvasiveDebugEnabled() is FALSE.</p> <p>When FEAT_Debugv8p4 is implemented, bit[23] of this register is <b>RES0</b>.</p>	0b00
[21]	TDA	<p>Traps accesses to the following debug System registers:</p> <ul style="list-style-type: none"> <li>AArch64: AArch64-DBGBCR&lt;n&gt;_EL1, AArch64-DBGBVR&lt;n&gt;_EL1, AArch64-DBGWCR&lt;n&gt;_EL1, AArch64-DBGWVR&lt;n&gt;_EL1.</li> </ul> <p><b>0b0</b></p> <p>Accesses to debug System registers do not generate a Software Access Debug event.</p> <p><b>0b1</b></p> <p>Accesses to debug System registers generate a Software Access Debug event, if AArch64-OSLSR_EL1.OSLK is 0 and if halting is allowed.</p> <p>When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers:</p> <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul>	0b0
[20]	MA	<p>Memory access mode. Controls the use of memory-access mode for accessing ITR and the DCC. This bit is ignored if in Non-debug state and set to zero on entry to Debug state.</p> <p>Possible values of this field are:</p> <p><b>0b0</b></p> <p>Normal access mode.</p> <p><b>0b1</b></p> <p>Memory access mode.</p>	0b0
[19]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[18]	NS	<p>Non-secure status. In Debug state, gives the current Security state:</p> <p><b>0b0</b> Secure state.</p> <p><b>0b1</b> Non-secure state.</p> <p><b>When !Halted()</b> Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b> Access to this field is: RO</p>	x
[17]	RES0	Reserved	RES0
[16]	SDD	<p>Secure debug disabled.</p> <p>On entry to Debug state:</p> <ul style="list-style-type: none"> <li>If entering in Secure state, SDD is set to 0.</li> <li>If entering in Non-secure state, SDD is set to the inverse of <code>ExternalSecureInvasiveDebugEnabled()</code>.</li> </ul> <p>In Debug state, the value of the SDD bit does not change, even if <code>ExternalSecureInvasiveDebugEnabled()</code> changes.</p> <p>In Non-debug state:</p> <ul style="list-style-type: none"> <li>SDD returns the inverse of <code>ExternalSecureInvasiveDebugEnabled()</code>. If the authentication signals that control <code>ExternalSecureInvasiveDebugEnabled()</code> change, a context synchronization event is required to guarantee their effect.</li> <li>This bit is unaffected by the Security state of the PE.</li> </ul> <p>Access to this field is: RO</p>	x
[15]	RES0	Reserved	RES0
[14]	HDE	<p>Halting debug enable.</p> <p><b>0b0</b> Halting disabled for Breakpoint, Watchpoint and Halt Instruction debug events.</p> <p><b>0b1</b> Halting enabled for Breakpoint, Watchpoint and Halt Instruction debug events.</p> <p>When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers:</p> <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul>	0b0

Bits	Name	Description	Reset
[13:10]	RW	<p>Exception level Execution state status. In Debug state, each bit gives the current Execution state of each Exception level.</p> <p><b>0b1111</b></p> <p>Any of the following:</p> <ul style="list-style-type: none"> <li>The PE is in Non-debug state.</li> <li>The PE is at EL0 using AArch64.</li> <li>The PE is not at EL0, and both EL1 and EL2 are using AArch64.</li> </ul> <p><b>When !Halted()</b></p> <p>Access to this field is: <b>RAO/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	0b1111
[9:8]	EL	<p>Exception level. In Debug state, gives the current Exception level of the PE.</p> <p><b>When !Halted()</b></p> <p>Access to this field is: <b>RAZ/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	xx
[7]	A	<p>SError interrupt pending. In Debug state, indicates whether an SError interrupt is pending:</p> <ul style="list-style-type: none"> <li>If AArch64-HCR_EL2.{AMO, TGE} = {1, 0}, EL2 is enabled in the current Security state, and the PE is executing at EL0 or EL1, a virtual SError interrupt.</li> <li>Otherwise, a physical SError interrupt.</li> </ul> <p><b>0b0</b></p> <p>No SError interrupt pending.</p> <p><b>0b1</b></p> <p>SError interrupt pending.</p> <p>A debugger can read EDSCR to check whether an SError interrupt is pending without having to execute further instructions. A pending SError might indicate data from target memory is corrupted.</p> <p><b>When !Halted()</b></p> <p>Access to this field is: <b>UNKNOWN/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	x
[6]	ERR	<p>Cumulative error flag. This bit is set to 1 following exceptions in Debug state and on any signaled overrun or underrun on the DTR or EDITR.</p> <p>When AArch64-OSLSR_EL1.OSLK is 1, this bit can be indirectly read and written through the following System registers:</p> <ul style="list-style-type: none"> <li>AArch64-MDSCR_EL1.</li> </ul> <p>Access to this field is: RO</p>	0b0

Bits	Name	Description	Reset
[5:0]	STATUS	<p>Debug status flags.</p> <p><b>0b000001</b> PE is restarting, exiting Debug state.</p> <p><b>0b000010</b> PE is in Non-debug state.</p> <p><b>0b000111</b> Breakpoint.</p> <p><b>0b010011</b> External debug request.</p> <p><b>0b011011</b> Halting step, normal.</p> <p><b>0b011111</b> Halting step, exclusive.</p> <p><b>0b100011</b> OS Unlock Catch.</p> <p><b>0b100111</b> Reset Catch.</p> <p><b>0b101011</b> Watchpoint.</p> <p><b>0b101111</b> HLT instruction.</p> <p><b>0b110011</b> Software access to debug register.</p> <p><b>0b110111</b> Exception Catch.</p> <p><b>0b111011</b> Halting step, no syndrome.</p> <p>All other values of STATUS are reserved.</p> <p>Access to this field is: RO</p>	6{x}

### Accessibility

Component	Offset	Instance	Range
Debug	0x088	EDSCR	None

This interface is accessible as follows:

**When IsCorePowered() and !OSLockStatus()**

RW

**Otherwise**

ERROR

B.2.2.1.7 DBGDTRTX\_EL0, Debug Data Transfer Register, Transmit

Transfers data from the PE to an external debugger. For example, it is used by a debug target to transfer data to the debugger. See AArch64-DBGDTR\_EL0 for additional architectural mappings. It is a component of the Debug Communication Channel.

Configurations

External register DBGDTRTX\_EL0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.21 DBGDTRTX\\_EL0, Debug Data Transfer Register, Transmit](#) on page 1118 bits [31:0].

Attributes

Width

32

Component

Debug

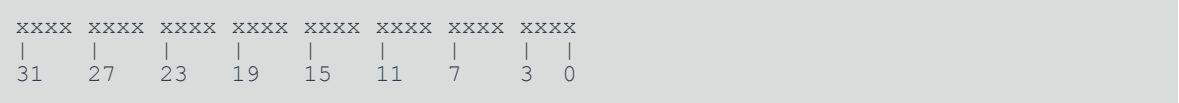
Register offset

0x08C

Access type

See bit descriptions

Reset value

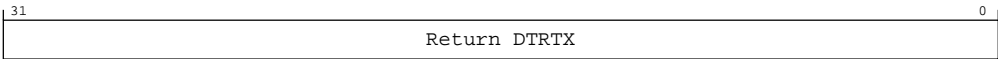


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-129: EXT\_DBGDTRTX\_EL0 bit assignments



**Table B-267: DBGDTRTX\_ELO bit descriptions**

Bits	Name	Description	Reset
[31:0]	None	<p>Return DTRTX.</p> <p>Reads of this register:</p> <ul style="list-style-type: none"> <li>If TXfull is set to 1, return the last value written to DTRTX.</li> <li>If TXfull is set to 0, return an <b>UNKNOWN</b> value.</li> </ul> <p>After the read, TXfull is cleared to 0.</p> <p>Writes to this register:</p> <ul style="list-style-type: none"> <li>If TXfull is set to 1, set DTRTX to <b>UNKNOWN</b>.</li> <li>If TXfull is set to 0, update the value in DTRTX.</li> </ul> <p>After the write, TXfull remains unchanged.</p> <p>For the full behavior of the Debug Communications Channel, see <i>The Debug Communication Channel and Instruction Transfer Register</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	32 {x}

### Access

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any operation issued by a DTR access in memory access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.
- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an **UNKNOWN** state.

### Accessibility

If ext-EDSCR.ITE == 0 when the PE exits Debug state on receiving a Restart request trigger event, the behavior of any operation issued by a DTR access in memory access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**, and must do one of the following:

- It must complete execution in Debug state before the PE executes the restart sequence.
- It must complete execution in Non-debug state before the PE executes the restart sequence.
- It must be abandoned. This means that the instruction does not execute. Any registers or memory accessed by the instruction are left in an **UNKNOWN** state.

Component	Offset	Instance	Range
Debug	0x08C	DBGDTRTX_ELO	None

This interface is accessible as follows:

#### When IsCorePowered() and !OSLockStatus()

RW

#### Otherwise

ERROR

B.2.2.1.8 EDRCR, External Debug Reserve Control Register

This register is used to allow imprecise entry to Debug state and clear sticky bits in ext-EDSCR.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

Debug

Register offset

0x090

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-130: EXT\_EDRCR bit assignments

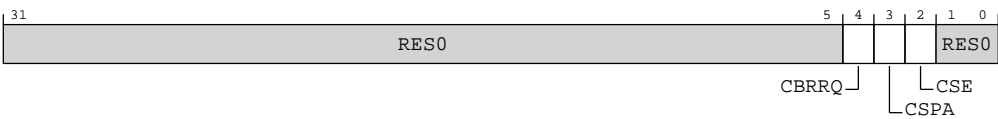


Table B-269: EDRCR bit descriptions

Bits	Name	Description	Reset
[31:5]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[4]	CBRRQ	<p>Allow imprecise entry to Debug state. The actions on writing to this bit are:</p> <p><b>0b0</b> No action.</p> <p><b>0b1</b> Allow imprecise entry to Debug state, for example by canceling pending bus accesses.</p> <p>Setting this bit to 1 allows a debugger to request imprecise entry to Debug state. An External Debug Request debug event must be pending before the debugger sets this bit to 1.</p>	x
[3]	CSPA	<p>Clear Sticky Pipeline Advance. This bit is used to clear the ext-EDSCR.PipeAdv bit to 0. The actions on writing to this bit are:</p> <p><b>0b0</b> No action.</p> <p><b>0b1</b> Clear the ext-EDSCR.PipeAdv bit to 0.</p>	x
[2]	CSE	<p>Clear Sticky Error. Used to clear the ext-EDSCR cumulative error bits to 0. The actions on writing to this bit are:</p> <p><b>0b0</b> No action.</p> <p><b>0b1</b> Clear the ext-EDSCR.{TXU, RXO, ERR} bits, and, if the PE is in Debug state, the ext-EDSCR.ITO bit, to 0.</p>	x
[1:0]	RES0	Reserved	RES0

## Accessibility

Component	Offset	Instance	Range
Debug	0x090	EDRCR	None

This interface is accessible as follows:

**When IsCorePowered() and !OSLockStatus()**

WO

**Otherwise**

ERROR

### B.2.2.1.9 EDECCR, External Debug Exception Catch Control Register

Controls Exception Catch debug events. For more information, see *Exception Catch debug event* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

## Configurations

External register EDECCR bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.5 OSECCR\\_EL1, OS Lock Exception Catch Control Register](#) on page 1081 bits [31:0].

Attributes

Width

32

Component

Debug

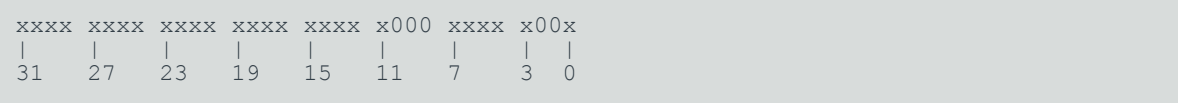
Register offset

0x098

Access type

RESORESO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-131: EXT\_EDECCR bit assignments

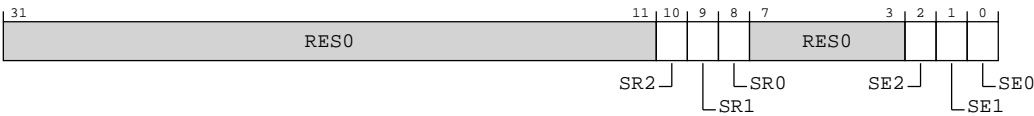


Table B-271: EDECCR bit descriptions

Bits	Name	Description	Reset
[31:11]	RES0	Reserved	RES0
[10]	SR2	Controls exception catch on exception return to Secure EL2 in conjunction with EDECCR.SE2.  <b>0b0</b>  If EDECCR.SE2 is 0, then Exception Catch debug events are disabled for Secure EL2.  If EDECCR.SE2 is 1, then Exception Catch debug events are enabled for exception entry, reset entry, and exception return to Secure EL2.  <b>0b1</b>  If EDECCR.SE2 is 0, then Exception Catch debug events are enabled for exception returns to Secure EL2.  If EDECCR.SE2 is 1, then Exception Catch debug events are enabled for exception entry and reset entry to Secure EL2.	0b0

Bits	Name	Description	Reset
[9]	SR1	Controls exception catch on exception return to Secure EL1 in conjunction with EDECCR.SE1.  <b>0b0</b> If EDECCR.SE1 is 0, then Exception Catch debug events are disabled for Secure EL1.  If EDECCR.SE1 is 1, then Exception Catch debug events are enabled for exception entry, reset entry, and exception return to Secure EL1.  <b>0b1</b> If EDECCR.SE1 is 0, then Exception Catch debug events are enabled for exception returns to Secure EL1.  If EDECCR.SE1 is 1, then Exception Catch debug events are enabled for exception entry and reset entry to Secure EL1.	0b0
[8]	SRO	Controls exception catch on exception return to Secure EL0.  <b>0b0</b> Exception Catch debug events are disabled for Secure EL0.  <b>0b1</b> Exception Catch debug events are enabled for exception returns to Secure EL0.	0b0
[7:3]	RES0	Reserved	RES0
[2]	SE2	Controls exception catch on exception entry to Secure EL2. Also controls exception catch on exception return to Secure EL2 in conjunction with EDECCR.SR2.  <b>0b0</b> If EDECCR.SR2 is 0, then Exception Catch debug events are disabled for Secure EL2.  If EDECCR.SR2 is 1, then Exception Catch debug events are enabled for exception returns to Secure EL2.  <b>0b1</b> If EDECCR.SR2 is 0, then Exception Catch debug events are enabled for exception entry, reset entry, and exception return to Secure EL2.  If EDECCR.SR2 is 1, then Exception Catch debug events are enabled for exception entry and reset entry to Secure EL2.  <b>Note:</b> It is <b>IMPLEMENTATION DEFINED</b> whether a reset entry to an Exception level will generate an Exception Catch debug event. In this implementation, a reset entry will do so.	0b0

Bits	Name	Description	Reset
[1]	SE1	<p>Controls exception catch on exception entry to Secure EL1. Also controls exception catch on exception return to Secure EL1 in conjunction with EDECCR.SR1.</p> <p><b>0b0</b></p> <p>If EDECCR.SR1 is 0, then Exception Catch debug events are disabled for Secure EL1.</p> <p>If EDECCR.SR1 is 1, then Exception Catch debug events are enabled for exception returns to Secure EL1.</p> <p><b>0b1</b></p> <p>If EDECCR.SR1 is 0, then Exception Catch debug events are enabled for exception entry, reset entry, and exception return to Secure EL1.</p> <p>If EDECCR.SR1 is 1, then Exception Catch debug events are enabled for exception entry and reset entry to Secure EL1.</p> <p><b>Note:</b> It is <b>IMPLEMENTATION DEFINED</b> whether a reset entry to an Exception level will generate an Exception Catch debug event. In this implementation, a reset entry will do so.</p>	0b0
[0]	SEO	None	x

## Accessibility

Component	Offset	Instance	Range
Debug	0x098	EDECCR	None

This interface is accessible as follows:

### When IsCorePowered() and !OSLockStatus()

RW

### Otherwise

ERROR

## B.2.2.1.10 OSLAR\_EL1, OS Lock Access Register

Used to lock or unlock the OS Lock.

## Configurations

External debug accesses to OSLAR\_EL1 are ignored and return an error when AllowExternalDebugAccess() returns FALSE for the access.

External register OSLAR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.11 OSLAR\\_EL1, OS Lock Access Register](#) on page 1099 bits [31:0].

## Attributes

### Width

32

Component

Debug

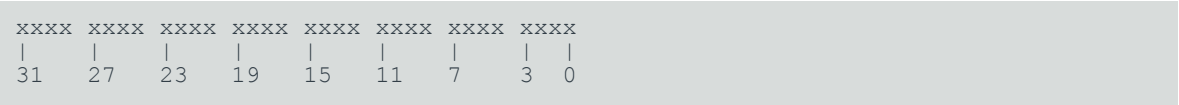
Register offset

0x300

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-132: EXT\_OSLAR\_EL1 bit assignments

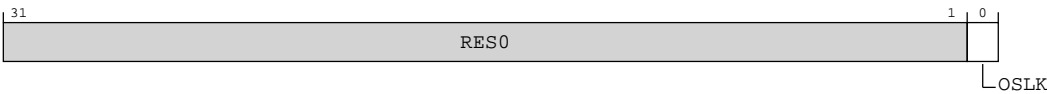


Table B-273: OSLAR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	OSLK	On writes to OSLAR_EL1, bit[0] is copied to the OS Lock.  Use ext-EDPRSR.OSLK to check the current status of the lock.	x

Accessibility

Component	Offset	Instance	Range
Debug	0x300	OSLAR_EL1	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalDebugAccess()**

WO

**Otherwise**

ERROR

B.2.2.1.11 EDPRCR, External Debug Power/Reset Control Register

Controls the PE functionality related to powerup, reset, and powerdown.

Configurations

All fields in this register are in the Core power domain.

CORENPDRQ is the only field that is mapped between the EDPRCR and DBGPRCR\_EL1.

Attributes

Width

32

Component

Debug

Register offset

0x310

Access type

inconsistent

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-133: EXT\_EDPRCR bit assignments

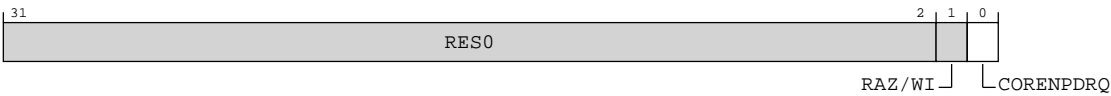


Table B-275: EDPRCR bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	RAZ/WI	Reserved	RAZ/ WI

Bits	Name	Description	Reset
[0]	CORENPDRQ	<p>Core no powerdown request. Requests emulation of powerdown.</p> <p>This request is typically passed to an external power controller. This means that whether a request causes power up is dependent on the <b>IMPLEMENTATION DEFINED</b> nature of the system. The power controller must not allow the Core power domain to switch off while this bit is 1.</p> <p><b>0b0</b></p> <p>If the system responds to a powerdown request, it powers down Core power domain.</p> <p><b>0b1</b></p> <p>If the system responds to a powerdown request, it does not powerdown the Core power domain, but instead emulates a powerdown of that domain.</p> <p>When this bit reads as <b>UNKNOWN</b>, the PE ignores writes to this bit.</p> <p>This field is in the Core power domain, and permitted accesses to this field map to the AArch64-DBGPRCR_EL1.CORENPDRQ field.</p> <p>This bit is not reset to the Cold reset value on exit from an IMPLEMENTATION DEFINED software-visible retention state.</p> <p><b>Note:</b> Writes to this bit are not prohibited by the IMPLEMENTATION DEFINED authentication interface. This means that a debugger can request emulation of powerdown regardless of whether invasive debug is permitted.</p> <p><b>When OSLockStatus()</b> Access to this field is: <b>UNKNOWN/WI</b></p> <p><b>Otherwise</b> Access to this field is: RW</p>	0b0

## Accessibility

On permitted accesses to the register, other access controls affect the behavior of some fields. See the field descriptions for more information.

Component	Offset	Instance	Range
Debug	0x310	EDPRCR	None

This interface is accessible as follows:

### When IsCorePowered()

RW

### Otherwise

ERROR

B.2.2.1.12 EDPRSR, External Debug Processor Status Register

Holds information about the reset and powerdown state of the PE.

Configurations

All fields in this register are in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0x314

Access type

inconsistent

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	x0x0	xxxx	1x11
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-134: EXT\_EDPRSR bit assignments

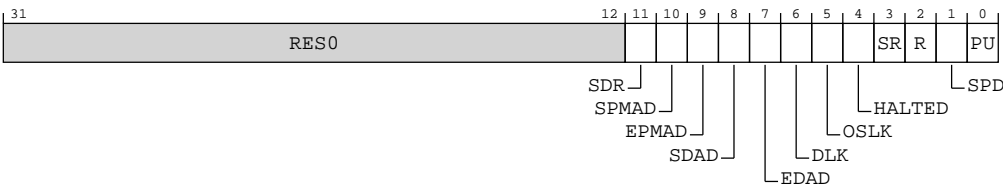


Table B-277: EDPRSR bit descriptions

Bits	Name	Description	Reset
[31:12]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[11]	SDR	<p>Sticky Debug Restart. Set to 1 when the PE exits Debug state.</p> <p>Permitted values are:</p> <p><b>0b0</b></p> <p>The PE has not restarted since EDPRSR was last read.</p> <p><b>0b1</b></p> <p>The PE has restarted since EDPRSR was last read.</p> <p><b>Note:</b></p> <p>If a reset occurs when the PE is in Debug state, the PE exits Debug state. SDR is <b>UNKNOWN</b> on Warm reset, meaning a debugger must also use the SR bit to determine whether the PE has left Debug state.</p> <p>If the Core power domain is powered up, then following a read of EDPRSR:</p> <ul style="list-style-type: none"> <li>This bit clears to 0.</li> </ul> <p>This field is in the Core power domain.</p> <p><b>When ext-EDPRSR.R == '1'</b></p> <p>Access to this field is: <b>UNKNOWN/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: <b>RC/WI</b></p>	x
[10]	SPMAD	<p>Sticky EPMAD error. Set to 1 if an external debug interface access to a Performance Monitors register returns an error because <code>AllowExternalPMUAccess() == FALSE</code>.</p> <p>Permitted values are:</p> <p><b>0b0</b></p> <p>No Non-secure external debug interface accesses to the external Performance Monitors registers have failed because <code>AllowExternalPMUAccess() == FALSE</code> for the access since EDPRSR was last read.</p> <p><b>0b1</b></p> <p>At least one Non-secure external debug interface access to the external Performance Monitors register has failed and returned an error because <code>AllowExternalPMUAccess() == FALSE</code> for the access since EDPRSR was last read.</p> <p>If the Core power domain is powered up, then following a read of EDPRSR:</p> <ul style="list-style-type: none"> <li>This bit clears to 0.</li> </ul> <p>This field is in the Core power domain.</p> <p><b>When ext-EDPRSR.R == '1'</b></p> <p>Access to this field is: <b>UNKNOWN/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: <b>RC/WI</b></p>	0b0

Bits	Name	Description	Reset
[9]	EPMAD	<p>External Performance Monitors Non-secure Access Disable status.</p> <p><b>0b0</b></p> <p>External Non-secure Performance Monitors access enabled. <code>AllowExternalPMUAccess()</code> == TRUE for a Non-secure access.</p> <p><b>0b1</b></p> <p>External Non-secure Performance Monitors access disabled. <code>AllowExternalPMUAccess()</code> == FALSE for a Non-secure access.</p> <p>This field is in the Core power domain.</p> <p><b>When ext-EDPRSR.R == '1'</b></p> <p>Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	x
[8]	SDAD	<p>Sticky EDAD error. Set to 1 if an external debug interface access to a debug register returns an error because <code>AllowExternalDebugAccess()</code> == FALSE.</p> <p><b>0b0</b></p> <p>No Non-secure external debug interface accesses to the debug registers have failed because <code>AllowExternalDebugAccess()</code> == FALSE for the access since EDPRSR was last read.</p> <p><b>0b1</b></p> <p>At least one Non-secure external debug interface access to the debug registers has failed and returned an error because <code>AllowExternalDebugAccess()</code> == FALSE for the access since EDPRSR was last read.</p> <p>If the Core power domain is powered up, then, following a read of EDPRSR:</p> <ul style="list-style-type: none"> <li>This bit clears to 0.</li> </ul> <p>This field is in the Core power domain.</p> <p><b>When ext-EDPRSR.R == '1'</b></p> <p>Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	0b0
[7]	EDAD	<p>External Debug Access Disable status.</p> <p><b>0b0</b></p> <p>External Non-secure access to breakpoint registers, watchpoint registers, and ext-OSLAR_EL1 enabled. <code>AllowExternalDebugAccess()</code> == TRUE for a Non-secure access.</p> <p><b>0b1</b></p> <p>External Non-secure access to breakpoint registers, watchpoint registers, and ext-OSLAR_EL1 disabled. <code>AllowExternalDebugAccess()</code> == FALSE for a Non-secure access.</p> <p>This field is in the Core power domain.</p> <p><b>When ext-EDPRSR.R == '1'</b></p> <p>Access to this field is: UNKNOWN/WI</p> <p><b>Otherwise</b></p> <p>Access to this field is: RO</p>	x
[6]	DLK	This field is <b>RES0</b> .	x

Bits	Name	Description	Reset
[5]	OSLK	<p>OS Lock status bit.</p> <p>A read of this bit returns the value of AArch64-OSLSR_EL1.OSLK.</p> <p>This field is in the Core power domain.</p> <p>Access to this field is: RO</p>	x
[4]	HALTED	<p>Halted status bit.</p> <p><b>0b0</b> PE is in Non-debug state.</p> <p><b>0b1</b> PE is in Debug state.</p> <p>This field is in the Core power domain.</p> <p>Access to this field is: RO</p>	x
[3]	SR	<p>Sticky core Reset status bit.</p> <p>Permitted values are:</p> <p><b>0b0</b> The non-debug logic of the PE is not in reset state and has not been reset since the last time EDPRSR was read.</p> <p><b>0b1</b> The non-debug logic of the PE is in reset state or has been reset since the last time EDPRSR was read.</p> <p>If EDPRSR.PU reads as 1 and EDPRSR.R reads as 0, which means that the Core power domain is in a powerup state and that the non-debug logic of the PE is not in reset state, then following a read of EDPRSR:</p> <ul style="list-style-type: none"> <li>This bit clears to 0.</li> </ul> <p>This field is in the Core power domain.</p> <p>Access to this field is: RC/<b>WI</b></p>	0b1
[2]	R	<p>PE Reset status bit.</p> <p>Permitted values are:</p> <p><b>0b0</b> The non-debug logic of the PE is not in reset state.</p> <p><b>0b1</b> The non-debug logic of the PE is in reset state.</p> <p>This field is in the Core power domain.</p> <p>Access to this field is: RO</p>	x

Bits	Name	Description	Reset
[1]	SPD	<p>Sticky core Powerdown status bit.</p> <p>For more information, see <i>EDPRSR.{DLK, SPD, PU}</i> and the Core power domain in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p><b>0b0</b></p> <p>If EDPRSR.PU is 0, it is not known whether the state of the debug registers in the Core power domain is lost.</p> <p>If EDPRSR.PU is 1, the state of the debug registers in the Core power domain has not been lost.</p> <p><b>0b1</b></p> <p>The state of the debug registers in the Core power domain has been lost.</p> <p>If the Core power domain is powered up, then, following a read of EDPRSR:</p> <ul style="list-style-type: none"> <li>This bit clears to 0.</li> </ul> <p>When <i>EDPRSR.SPD</i> when the Core domain is in either retention or powerdown state in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>EDPRSR.{DLK, SPD, PU} describe whether registers in the Core power domain can be accessed, and whether their state has been lost since the last time the register was read. For more information, see <i>EDPRSR.{DLK, SPD, PU}</i> and the Core power domain in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>This field is in the Core power domain.</p> <p>Access to this field is: RO</p>	0b1
[0]	PU	<p>Core powerup status bit.</p> <p>Access to this field is: <b>RAO/WI</b></p>	0b1

## Access

On permitted accesses to the register, other access controls affect the behavior of some fields. See the field descriptions for more information.

If the Core power domain is powered up (EDPRSR.PU == 1), then following a read of EDPRSR:

- EDPRSR.{SDR, SPMAD, SDAD, SPD} are cleared to 0.
- EDPRSR.SR is cleared to 0 if the non-debug logic of the PE is not in reset state (EDPRSR.R == 0).

The clearing of bits is an indirect write to EDPRSR.

## Accessibility

On permitted accesses to the register, other access controls affect the behavior of some fields. See the field descriptions for more information.

If the Core power domain is powered up (EDPRSR.PU == 1), then following a read of EDPRSR:

- EDPRSR.{SDR, SPMAD, SDAD, SPD} are cleared to 0.

- EDPRSR.SR is cleared to 0 if the non-debug logic of the PE is not in reset state (EDPRSR.R == 0).

The clearing of bits is an indirect write to EDPRSR.

Component	Offset	Instance	Range
Debug	0x314	EDPRSR	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.1.13 DBGBVR<n>\_EL1, Debug Breakpoint Value Registers, n = 0 - 5

Holds a virtual address, or a VMID and/or a context ID, for use in breakpoint matching. Forms breakpoint n together with control register ext-DBGBCR<n>\_EL1.

Configurations

How this register is interpreted depends on the value of ext-DBGBCR<n>\_EL1.BT.

- When ext-DBGBCR<n>\_EL1.BT is 0b0x0x, this register holds a virtual address.
- When ext-DBGBCR<n>\_EL1.BT is 0b001x, 0b011x, or 0b110x, this register holds a Context ID.
- When ext-DBGBCR<n>\_EL1.BT is 0b100x, this register holds a VMID.
- When ext-DBGBCR<n>\_EL1.BT is 0b101x, this register holds a VMID and a Context ID.
- When ext-DBGBCR<n>\_EL1.BT is 0b111x, this register holds two Context ID values.

For other values of ext-DBGBCR<n>\_EL1.BT, this register is RES0.

If breakpoint n is not implemented then accesses to this register are:

- RES0 when IsCorePowered() && !OSLockStatus() && AllowExternalDebugAccess().
- ERROR otherwise.

External register DBGBVR<n>\_EL1 bits [63:0] are architecturally mapped to AArch64 System register [A.2.5.6 DBGBVR<n>\\_EL1, Debug Breakpoint Value Registers, n = 0 - 5](#) on page 1083 bits [63:0].

Attributes

**Width**

64

**Component**

Debug

Register offset

0x400 + (16 \* n)

Access type

See bit descriptions

Reset value

- When `ext-DBGBCR<n>_EL1.BT == '0x0x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '001x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '011x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '100x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '101x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '110x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
- When `ext-DBGBCR<n>_EL1.BT == '111x'`  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

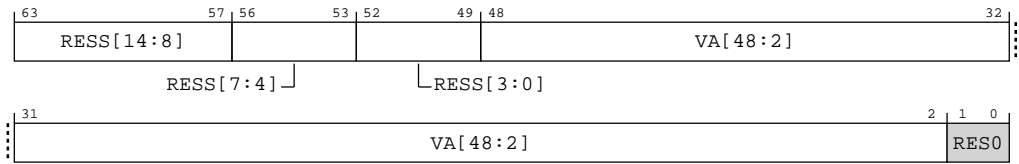


Where the reset reads xxxx, see individual bits.

Bit descriptions

When `ext-DBGBCR<n>_EL1.BT == '0x0'`

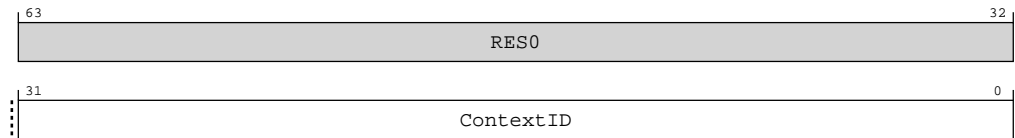
Figure B-135: EXT\_DBGBCR<n>\_EL1 bit assignments



**Table B-279: DBGBCR<n>\_EL1 bit descriptions**

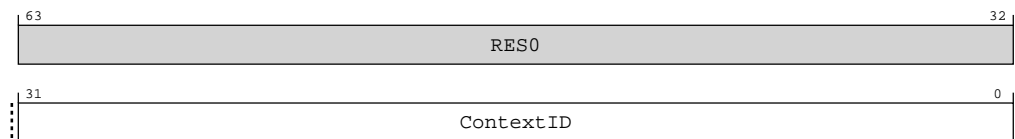
Bits	Name	Description	Reset
[63:57]	RESS[14:8]	Reserved, Sign extended. Hardware and software must treat this field as <b>RES0</b> if the most significant bit of VA is 0 or <b>RES0</b> , and as RES1 if the most significant bit of VA is 1. Hardware always ignores the value of these bits and the bits are hardwired to a copy of the most significant bit of VA, meaning writes to these bits are ignored, and reads to the bits always return the hardwired value.	7 {x}
[56:53]	RESS[7:4]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[52:49]	RESS[3:0]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[48:2]	VA[48:2]	If the address is being matched in an AArch64 stage 1 translation regime: <ul style="list-style-type: none"> <li>This field contains bits[48:2] of the address for comparison.</li> </ul>	47 {x}
[1:0]	<b>RES0</b>	Reserved	<b>RES0</b>

When ext-DBGBCR<n>\_EL1.BT == '001'

**Figure B-136: EXT\_DBGBCR<n>\_EL1 bit assignments****Table B-280: DBGBCR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	ContextID	Context ID value for comparison.  The value is compared against the following: <ul style="list-style-type: none"> <li>AArch64-CONTEXTIDR_EL1 when the PE is executing at AArch64.</li> </ul>	32 {x}

When ext-DBGBCR<n>\_EL1.BT == '011'

**Figure B-137: EXT\_DBGBCR<n>\_EL1 bit assignments****Table B-281: DBGBCR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:32]	<b>RES0</b>	Reserved	<b>RES0</b>
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32 {x}

When ext-DBGBCR<n>\_EL1.BT == '100'

Figure B-138: EXT\_DBGBVR<n>\_EL1 bit assignments

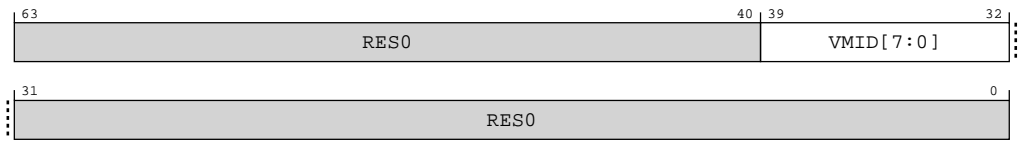


Table B-282: DBGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	VMID[7:0]	VMID value for comparison.	8 {x}
[31:0]	RES0	Reserved	RES0

When ext-DBGBCR<n>\_EL1.BT == '101'

Figure B-139: EXT\_DBGBVR<n>\_EL1 bit assignments

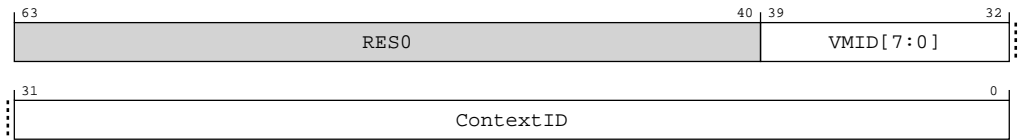


Table B-283: DBGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:40]	RES0	Reserved	RES0
[39:32]	VMID[7:0]	VMID value for comparison.	8 {x}
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32 {x}

When ext-DBGBCR<n>\_EL1.BT == '110'

Figure B-140: EXT\_DBGBVR<n>\_EL1 bit assignments

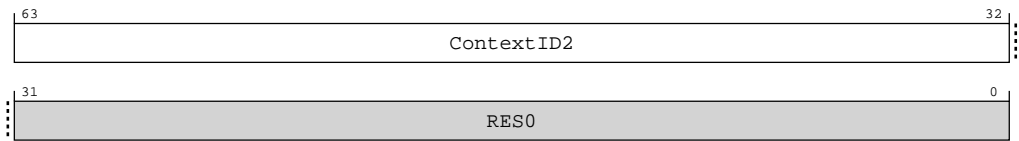


Table B-284: DBGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	ContextID2	Context ID value for comparison against AArch64-CONTEXTIDR_EL2.	32 {x}
[31:0]	RES0	Reserved	RES0

When ext-DBGBCR<n>\_EL1.BT == '111'



Figure B-141: EXT\_DBGBVR<n>\_EL1 bit assignments

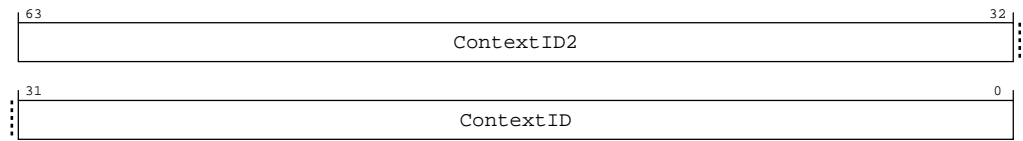


Table B-285: DBGBVR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:32]	ContextID2	Context ID value for comparison against AArch64-CONTEXTIDR_EL2.	32 { x }
[31:0]	ContextID	Context ID value for comparison against AArch64-CONTEXTIDR_EL1.	32 { x }

Accessibility

Component	Offset	Instance	Range
Debug	0x400 + (16 * n)	DBGBVR<n>_EL1	63:0

This interface is accessible as follows:

**When IsCorePowered(), !OSLockStatus() and AllowExternalDebugAccess()**  
RW

**Otherwise**  
ERROR

B.2.2.1.14 DBGBCR<n>\_EL1, Debug Breakpoint Control Registers, n = 0 - 5

Holds control information for a breakpoint. Forms breakpoint n together with value register ext-DBGBVR<n>\_EL1.

Configurations

- If breakpoint n is not implemented then accesses to this register are:
- RES0 when IsCorePowered() && !OSLockStatus() && AllowExternalDebugAccess().
  - ERROR otherwise.

External register DBGBCR<n>\_EL1 bits [63:0] are architecturally mapped to AArch64 System register [A.2.5.7 DBGBCR<n>\\_EL1, Debug Breakpoint Control Registers, n = 0 - 5](#) on page 1088 bits [63:0].

Attributes

Width

64

Component

Debug

Register offset

$0x408 + (16 * n)$

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

When the E field is zero, all the other fields in the register are ignored.

Figure B-142: EXT\_DBGBCR<n>\_EL1 bit assignments

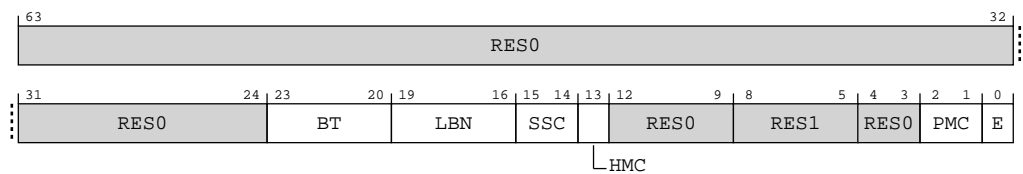


Table B-287: DBGBCR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:24]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[23:20]	BT	<p>Breakpoint Type.</p> <p>Specifies breakpoint type.</p> <p><b>0b0000</b> Unlinked instruction address match. ext-DBGBVR&lt;n&gt;_EL1 is the address of an instruction.</p> <p><b>0b0001</b> Linked instruction address match. As 0b0000, but linked to a breakpoint that has linking enabled.</p> <p><b>0b0010</b> Unlinked Context ID match. When FEAT_VHE is implemented, EL2 is using AArch64, the Effective value of AArch64-HCR_EL2.E2H is 1, and either the PE is executing at EL0 with AArch64-HCR_EL2.TGE set to 1 or the PE is executing at EL2, then ext-DBGBVR&lt;n&gt;_EL1.ContextID must match the AArch64-CONTEXTIDR_EL2 value. Otherwise, ext-DBGBVR&lt;n&gt;_EL1.ContextID must match the AArch64-CONTEXTIDR_EL1 value.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b0011</b> As 0b0010, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1000</b> Unlinked VMID match. ext-DBGBVR&lt;n&gt;_EL1.VMID is a VMID compared against AArch64-VTTBR_EL2.VMID.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1001</b> As 0b1000, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1010</b> Unlinked VMID and Context ID match. ext-DBGBVR&lt;n&gt;_EL1.ContextID is a Context ID compared against AArch64-CONTEXTIDR_EL1, and ext-DBGBVR&lt;n&gt;_EL1.VMID is a VMID compared against AArch64-VTTBR_EL2.VMID.</p> <p>This value applies when breakpoint n is context-aware.</p> <p><b>0b1011</b> As 0b1010, with linking enabled.</p> <p>This value applies when breakpoint n is context-aware.</p>	xxxx
[19:16]	LBN	<p>Linked Breakpoint Number.</p> <p>For Linked address matching breakpoints, specifies the index of the breakpoint linked to.</p> <p>For all other breakpoint types, this field is ignored and reads of the register return an <b>UNKNOWN</b> value.</p>	xxxx

Bits	Name	Description	Reset
[15:14]	SSC	Security state control. Determines the Security states under which a Breakpoint debug event for breakpoint n is generated. This field must be interpreted along with the HMC and PMC fields, and there are constraints on the permitted values of the {HMC, SSC, PMC} fields. For more information, including the effect of programming the fields to a reserved set of values, see <i>Reserved DBGBCR&lt;n&gt;_EL1.{SSC, HMC, PMC} values</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .  For more information on the operation of the SSC, HMC, and PMC fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	xx
[13]	HMC	Higher mode control. Determines the debug perspective for deciding when a Breakpoint debug event for breakpoint n is generated. This field must be interpreted along with the SSC and PMC fields, and there are constraints on the permitted values of the {HMC, SSC, PMC} fields. For more information see ext-DBGBCR<n>_EL1.SSC description.  For more information on the operation of the SSC, HMC, and PMC fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x
[12:9]	RES0	Reserved	RES0
[8:5]	RES1	Reserved	RES1
[4:3]	RES0	Reserved	RES0
[2:1]	PMC	Privilege mode control. Determines the Exception level or levels at which a Breakpoint debug event for breakpoint n is generated. This field must be interpreted along with the SSC and HMC fields, and there are constraints on the permitted values of the {HMC, SSC, PMC} fields. For more information see the ext-DBGBCR<n>_EL1.SSC description.  For more information on the operation of the SSC, HMC, and PMC fields, see <i>Execution conditions for which a breakpoint generates Breakpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	xx
[0]	E	Enable breakpoint n.  <b>0b0</b> Breakpoint n disabled.  <b>0b1</b> Breakpoint n enabled.	x

## Accessibility

Component	Offset	Instance	Range
Debug	0x408 + (16 * n)	DBGBCR<n>_EL1	None

This interface is accessible as follows:

**When IsCorePowered(), !OSLockStatus() and AllowExternalDebugAccess()**

RW

**Otherwise**

ERROR

B.2.2.1.15    DBGWVR<n>\_EL1, Debug Watchpoint Value Registers, n = 0 - 3

Holds a data address value for use in watchpoint matching. Forms watchpoint n together with control register ext-DBGWCR<n>\_EL1.

Configurations

If watchpoint n is not implemented then accesses to this register are:

- RES0 when IsCorePowered() && !OSLockStatus() && AllowExternalDebugAccess().
- ERROR otherwise.

External register DBGWVR<n>\_EL1 bits [63:0] are architecturally mapped to AArch64 System register A.2.5.8 DBGWVR<n>\_EL1, Debug Watchpoint Value Registers, n = 0 - 3 on page 1091 bits [63:0].

Attributes

Width

64

Component

Debug

Register offset

0x800 + (16 \* n)

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	0

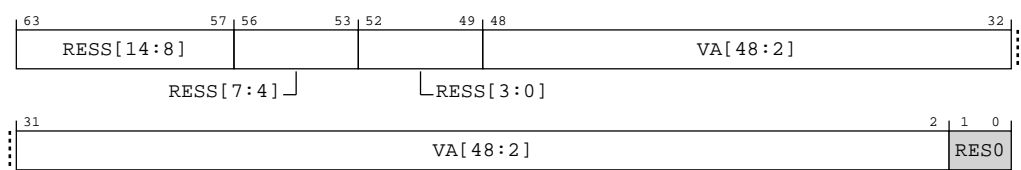


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-143: EXT\_DBGWVR<n>\_EL1 bit assignments



**Table B-289: DBGWVR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[63:57]	RESS[14:8]	Reserved, Sign extended. Hardware and software must treat this field as <b>RES0</b> if the most significant bit of VA is 0 or <b>RES0</b> , and as RES1 if the most significant bit of VA is 1. Hardware always ignores the value of these bits and the bits are hardwired to a copy of the most significant bit of VA, meaning writes to these bits are ignored, and reads to the bits always return the hardwired value.	7 {x}
[56:53]	RESS[7:4]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[52:49]	RESS[3:0]	Extension to RESS[14:8]. For more information, see RESS[14:8].	xxxx
[48:2]	VA[48:2]	Bits[48:2] of the address value for comparison.  Arm deprecates setting ext-DBGWVR<n>_EL1[2] == 1.	4 7 {x}
[1:0]	<b>RES0</b>	Reserved	<b>RES0</b>

### Accessibility

Component	Offset	Instance	Range
Debug	0x800 + (16 * n)	DBGWVR<n>_EL1	63:0

This interface is accessible as follows:

**When IsCorePowered(), !OSLockStatus() and AllowExternalDebugAccess()**

RW

**Otherwise**

ERROR

#### B.2.2.1.16 DBGWCR<n>\_EL1, Debug Watchpoint Control Registers, n = 0 - 3

Holds control information for a watchpoint. Forms watchpoint n together with value register ext-DBGWVR<n>\_EL1.

### Configurations

If watchpoint n is not implemented then accesses to this register are:

- RES0 when IsCorePowered() && !OSLockStatus() && AllowExternalDebugAccess().
- ERROR otherwise.

External register DBGWCR<n>\_EL1 bits [63:0] are architecturally mapped to AArch64 System register [A.2.5.9 DBGWCR<n>\\_EL1, Debug Watchpoint Control Registers, n = 0 - 3](#) on page 1093 bits [63:0].

### Attributes

#### Width

64

#### Component

Debug

Register offset

$0x808 + (16 * n)$

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

When the E field is zero, all the other fields in the register are ignored.

Figure B-144: EXT\_DBGWCR<n>\_EL1 bit assignments

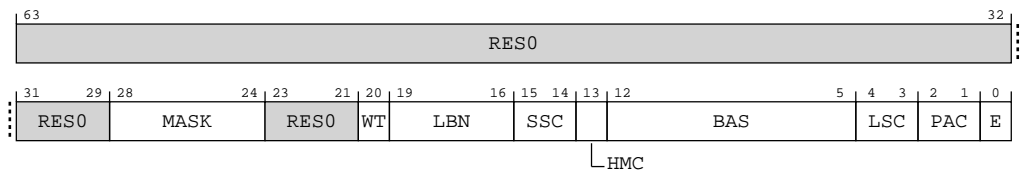


Table B-291: DBGWCR<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:29]	RES0	Reserved	RES0
[28:24]	MASK	Address Mask. Only objects up to 2GB can be watched using a single mask.  0b00000 No mask.  All other values are reserved.  Indicates the number of masked address bits, from 0b00011 masking 3 address bits (0x00000007 mask for address) to 0b11111 masking 31 address bits (0x7FFFFFFF mask for address).  If programmed with a reserved value, the watchpoint behaves as if either: <ul style="list-style-type: none"><li>DBGWCR&lt;n&gt;_EL1.MASK has been programmed with a defined value, which might be 0 (no mask), other than for a direct read of DBGWCR&lt;n&gt;_EL1.</li><li>The watchpoint is disabled.</li></ul>	5 {x}
[23:21]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[20]	WT	Watchpoint type. Possible values are:  <b>0b0</b> Unlinked data address match.  <b>0b1</b> Linked data address match.	x
[19:16]	LBN	Linked Breakpoint Number.  For Linked data address watchpoints, specifies the index of the breakpoint linked to.  For all other watchpoint types, this field is ignored and reads of the register return an <b>UNKNOWN</b> value.	xxxx
[15:14]	SSC	Security state control. Determines the Security states under which a Watchpoint debug event for watchpoint n is generated. This field must be interpreted along with the HMC and PAC fields.  For more information on the operation of the SSC, HMC, and PAC fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	xx
[13]	HMC	Higher mode control. Determines the debug perspective for deciding when a Watchpoint debug event for watchpoint n is generated. This field must be interpreted along with the SSC and PAC fields.  For more information on the operation of the SSC, HMC, and PAC fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	x
[12:5]	BAS	Byte address select. Each bit of this field selects whether a byte from within the word or double-word addressed by ext-DBGWVR<n>_EL1 is being watched. <a href="#">Table B-292: BAS description</a> on page 1765  In cases where ext-DBGWVR<n>_EL1 addresses a double-word: <a href="#">Table B-293: BAS description table 2</a> on page 1765  If ext-DBGWVR<n>_EL1[2] == 1, only BAS[3:0] is used. Arm deprecates setting ext-DBGWVR<n>_EL1[2] == 1.  The valid values for BAS are nonzero binary number all of whose set bits are contiguous. All other values are reserved and must not be used by software. See <i>Reserved DBGWCR&lt;n&gt;.BAS values</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	8 {x}
[4:3]	LSC	Load/store control. This field enables watchpoint matching on the type of access being made. Possible values of this field are:  <b>0b01</b> Match instructions that load from a watchpointed address.  <b>0b10</b> Match instructions that store to a watchpointed address.  <b>0b11</b> Match instructions that load from or store to a watchpointed address.  All other values are reserved, but must behave as if the watchpoint is disabled. Software must not rely on this property as the behavior of reserved values might change in a future revision of the architecture.	xx
[2:1]	PAC	Privilege of access control. Determines the Exception level or levels at which a Watchpoint debug event for watchpoint n is generated. This field must be interpreted along with the SSC and HMC fields.  For more information on the operation of the SSC, HMC, and PAC fields, see <i>Execution conditions for which a watchpoint generates Watchpoint exceptions</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a> .	xx



Bits	Name	Description	Reset
[0]	E	Enable watchpoint n.  <b>0b0</b> Watchpoint n disabled.  <b>0b1</b> Watchpoint n enabled.	x

**Table B-292: BAS description**

BAS	Description
xxxxxxx1	Match byte at AArch64-DBGWVR<n>_EL1
xxxxxx1x	Match byte at AArch64-DBGWVR<n>_EL1 + 1
xxxxx1xx	Match byte at AArch64-DBGWVR<n>_EL1 + 2
xxxx1xxx	Match byte at AArch64-DBGWVR<n>_EL1 + 3

**Table B-293: BAS description table 2**

BAS	Description, if AArch64-DBGWVR<n>_EL1[2] == 0
xxx1xxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 4
xx1xxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 5
x1xxxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 6
1xxxxxxx	Match byte at AArch64-DBGWVR<n>_EL1 + 7

## Accessibility

Component	Offset	Instance	Range
Debug	0x808 + (16 * n)	DBGWCR<n>_EL1	None

This interface is accessible as follows:

**When IsCorePowered(), !OSLockStatus() and AllowExternalDebugAccess()**

RW

**Otherwise**

ERROR

### B.2.2.1.17 MIDR\_EL1, Main ID Register

Provides identification information for the PE, including an implementer code for the device and a device ID number.

## Configurations

External register MIDR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.1.1 MIDR\\_EL1, Main ID Register](#) on page 332 bits [31:0].

Attributes

Width

32

Component

Debug

Register offset

0xD00

Access type

See bit descriptions

Reset value

0100 0001 0000 1111 1101 0001 0100 0001

Bit descriptions

Figure B-145: EXT\_MIDR\_EL1 bit assignments

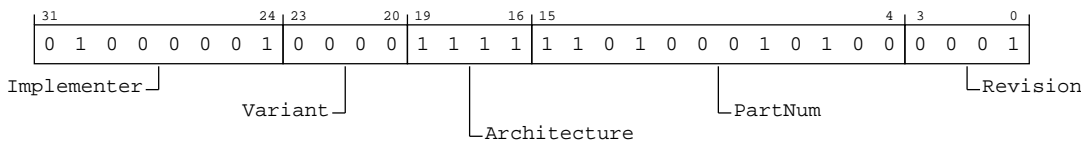


Table B-295: MIDR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:24]	Implementer	The Implementer code. This field must hold an implementer code that has been assigned by Arm. <b>0b01000001</b> Arm Limited	0x41
[23:20]	Variant	The major product revision variant number. <b>0b0000</b> r0.	0b0000
[19:16]	Architecture	Architecture version. Defined values are: <b>0b1111</b> Architectural features are individually identified in the ID_* registers. All other values are reserved.	0b1111
[15:4]	PartNum	The primary part number for the device. <b>0b110100010100</b> Cortex-R82AE.	0xD14
[3:0]	Revision	The minor product revision variant number. <b>0b0001</b> p1.	0b0001

Accessibility

Component	Offset	Instance	Range
Debug	0xD00	MIDR_EL1	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ImplementationDefined

B.2.2.1.18 EDPFR, External Debug Processor Feature Register

Provides information about implemented PE features.

For general information about the interpretation of the ID registers, see 'Principles of the ID scheme for fields in ID registers' in the Arm® Architecture Reference Manual, Armv8, for Armv8-A architecture profile.

Configurations

This register is available in all configurations.

Attributes

**Width**

64

**Component**

Debug

**Register offsets (2)**

0xD20,0xD24

**Access type**

See bit descriptions

**Reset value**

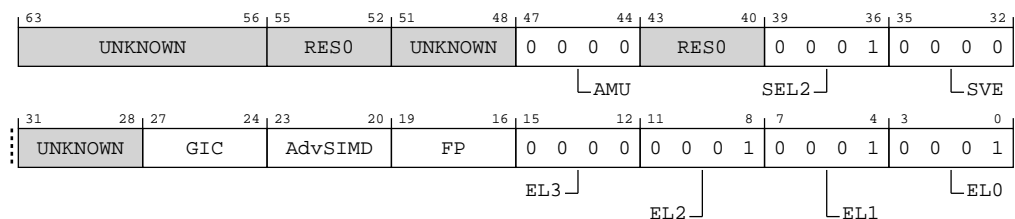
xxxx	xxxx	xxxx	xxxx	0000	xxxx	0001	0000	xxxx	xxxx	xxxx	xxxx	0000	0001	0001	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-146: EXT\_EDPFR bit assignments**



**Table B-297: EDPFR bit descriptions**

Bits	Name	Description	Reset
[63:56]	UNKNOWN	Reserved	UNKNOWN
[55:52]	RES0	Reserved	RES0
[51:48]	51:48	<b>When Variant(v8Ap4)</b> RES0  <b>Otherwise</b> RES0	xxxx
[47:44]	AMU	Activity Monitors Extension.  <b>0b0000</b> Activity Monitors Extension is not implemented.	0b0000
[43:40]	RES0	Reserved	RES0
[39:36]	SEL2	Secure EL2.  <b>0b0001</b> Secure EL2 is implemented.	0b0001
[35:32]	SVE	Scalable Vector Extension.  <b>0b0000</b> SVE architectural state and programmers' model are not implemented.	0b0000
[31:28]	UNKNOWN	Reserved	UNKNOWN
[27:24]	GIC	<b>When GICCDISABLE == 0</b> System register GIC interface support.  <b>0001</b> GIC CPU interface enabled. System register interface to versions 3.0 and 4.0 of the GIC CPU interface is supported.  <b>Otherwise</b> System register GIC interface support.  <b>0000</b> GIC CPU interface disabled. System register interface to any external GIC not supported.	xxxx

Bits	Name	Description	Reset
[23:20]	AdvSIMD	<b>When NEON_FPm &gt; 0</b> Advanced SIMD. <b>0001</b> Advanced SIMD is implemented that includes the FEAT_FP16 extension.  <b>Otherwise</b> Advanced SIMD. <b>1111</b> Advanced SIMD is not implemented.	xxxx
[19:16]	FP	<b>When NEON_FPm &gt; 0</b> Floating-point. <b>0001</b> Floating-point is implemented that includes the FEAT_FP16 extension.  <b>Otherwise</b> Floating-point. <b>1111</b> Floating-point is not implemented.	xxxx
[15:12]	EL3	EL3 Exception level handling. <b>0b0000</b> EL3 is not implemented.	0b0000
[11:8]	EL2	EL2 Exception level handling. <b>0b0001</b> EL2 can be executed in AArch64 state only.	0b0001
[7:4]	EL1	EL1 Exception level handling. <b>0b0001</b> EL1 can be executed in AArch64 state only.	0b0001
[3:0]	ELO	ELO Exception level handling. <b>0b0001</b> ELO can be executed in AArch64 state only.	0b0001

## Accessibility

Component	Offset	Instance	Range
Debug	0xD20	EDPFR	31:0

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

Component	Offset	Instance	Range
Debug	0xD24	EDPFR	63:32

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.1.19 EDDFR, External Debug Feature Register

Provides top level information about the debug system.

Debuggers must use ext-EDDEVARCH to determine the Debug architecture version. For general information about the interpretation of the ID registers, see 'Principles of the ID scheme for fields in ID registers' in the Arm® Architecture Reference Manual, Armv8, for Armv8-A architecture profile.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

Debug

Register offsets (2)

0xD28,0xD2C

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	0001	xxxx	xxxx	0001	xxxx	0011	xxxx	0101	0101	0001	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

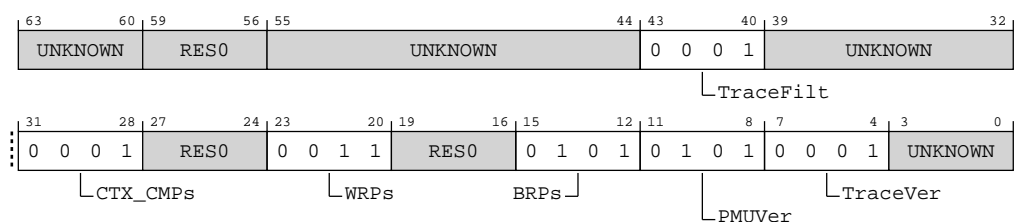


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-147: EXT\_EDDFR bit assignments**



**Table B-300: EDDFR bit descriptions**

Bits	Name	Description	Reset
[63:60]	UNKNOWN	Reserved	UNKNOWN
[59:56]	RES0	Reserved	RES0
[55:44]	UNKNOWN	Reserved	UNKNOWN
[43:40]	TraceFilt	Armv8.4 Self-hosted Trace Extension version. <b>0b0001</b> Armv8.4 Self-hosted Trace Extension implemented.	0b0001
[39:32]	UNKNOWN	Reserved	UNKNOWN
[31:28]	CTX_CMPs	Number of breakpoints that are context-aware, minus 1. These are the highest numbered breakpoints. <b>0b0001</b> 2 context-aware breakpoints implemented.	0b0001
[27:24]	RES0	Reserved	RES0
[23:20]	WRPs	Number of watchpoints, minus 1. <b>0b0011</b> 4 watchpoints implemented.	0b0011
[19:16]	RES0	Reserved	RES0
[15:12]	BRPs	Number of breakpoints, minus 1. <b>0b0101</b> 6 breakpoints implemented.	0b0101
[11:8]	PMUVer	Performance Monitors Extension version. <b>0b0101</b> PMUv3 for Armv8.4.	0b0101
[7:4]	TraceVer	Trace support. Indicates whether System register interface to a PE trace unit is implemented. <b>0b0001</b> PE trace unit System registers implemented.	0b0001
[3:0]	UNKNOWN	Reserved	UNKNOWN

## Accessibility

Component	Offset	Instance	Range
Debug	0xD28	EDDFR	31:0

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

Component	Offset	Instance	Range
Debug	0xD2C	EDDFR	63:32

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.1.20 EDAA32PFR, External Debug Auxiliary Processor Feature Register

Provides information about implemented PE features.



The register mnemonic, EDAA32PFR, is derived from previous definitions of this register that defined this register only when AArch64 was not supported.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

Debug

Register offset

0xD60

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000	0000	1111



63 59 55 51 47 43 39 35 31 27 23 19 15 11 7 3 0

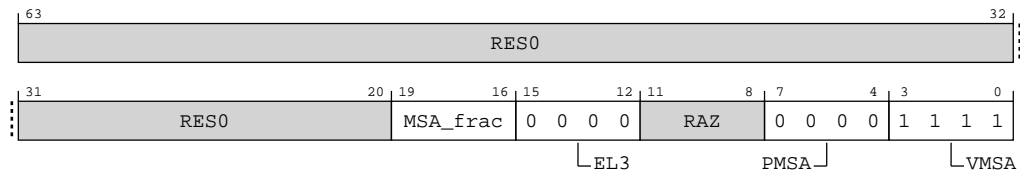


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-148: EXT\_EDAA32PFR bit assignments**



**Table B-303: EDAA32PFR bit descriptions**

Bits	Name	Description	Reset
[63:20]	RES0	Reserved	RES0
[19:16]	MSA_frac	<p><b>When VMSAm == 1</b></p> <p>Memory System Architecture fractional field. This holds information on additional Memory System Architectures supported.</p> <p><b>0010</b></p> <p>PMSAv8-64 supported in all translation regimes. In addition to PMSAv8-64, stage 1 EL1&amp;0 transaltion regime also supports VMSAv8-64.</p> <p><b>Otherwise</b></p> <p>Memory System Architecture fractional field. This holds information on additional Memory System Architectures supported.</p> <p><b>0001</b></p> <p>PMSAv8-64 supported in all translation regimes. VMSAv8-64 not supported.</p>	xxxx
[15:12]	EL3	<p>AArch32 EL3 Exception level handling. Defined values are:</p> <p><b>0b0000</b></p> <p>EL3 is not implemented or can be executed in AArch64 state.</p>	0b0000
[11:8]	RAZ	Reserved	RAZ
[7:4]	PMSA	<p>Indicates support for a 32-bit PMSA. Defined values are:</p> <p><b>0b0000</b></p> <p>PMSA-32 not supported.</p> <p>All other values are reserved.</p>	0b0000

Bits	Name	Description	Reset
[3:0]	VMSA	Defined values are:  <b>0b1111</b> Memory system architecture described by EDAA32PFR.MSA_frac.  All other values are reserved.  In Armv8-R AArch64, the only permitted value is 0b1111.	0b1111

Accessibility

Component	Offset	Instance	Range
Debug	0xD60	EDAA32PFR	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ImplementationDefined

B.2.2.1.21 EDITCTRL, External Debug Integration mode Control register

Enables the external debug to switch from its default mode into integration mode, where test software can control directly the inputs and outputs of the PE, for integration testing or topology detection.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xF00

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx0
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-149: EXT\_EDITCTRL bit assignments

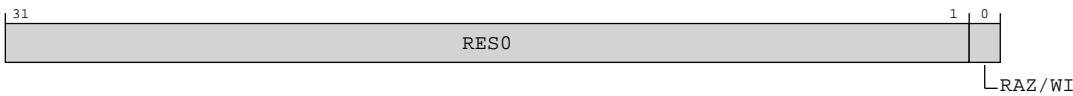


Table B-305: EDITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Instance	Range
Debug	0xF00	EDITCTRL	None

This interface is accessible as follows:

When IsCorePowered() and !OSLockStatus()

RW

Otherwise

ImplementationDefined

B.2.2.1.22 DBGCLAIMSET\_EL1, Debug CLAIM Tag Set Register

Used by software to set the CLAIM tag bits to 1.

The architecture does not define any functionality for the CLAIM tag bits.



CLAIM tags are typically used for communication between the debugger and target software.

Used in conjunction with the ext-DBGCLAIMCLR\_EL1 register.

Configurations

An implementation must include eight CLAIM tag bits.

External register DBGCLAIMSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.15 DBGCLAIMSET\\_EL1, Debug CLAIM Tag Set Register](#) on page 1106 bits [31:0].

Attributes

Width

32

Component

Debug

Register offset

0xFA0

Access type

RAOW1S

Reset value

0000 0000 0000 0000 0000 0000 1111 1111

Bit descriptions

Figure B-150: EXT\_DBGCLAIMSET\_EL1 bit assignments

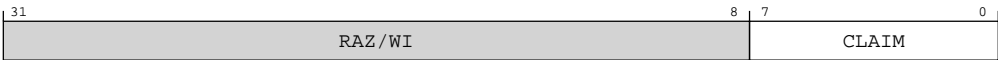


Table B-307: DBGCLAIMSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RAZ/WI	Reserved	RAZ/ WI
[7:0]	CLAIM	Set CLAIM tag bits.  This field is <b>RAO</b> .  Writing a 1 to one of these bits sets the corresponding CLAIM tag bit to 1. This is an indirect write to the CLAIM tag bits. A single write operation can set multiple CLAIM tag bits to 1.  Writing 0 to one of these bits has no effect.	0xFF

Accessibility

Component	Offset	Instance	Range
Debug	0xFA0	DBGCLAIMSET_EL1	None

This interface is accessible as follows:

When IsCorePowered() and !OSLockStatus()

RW

Otherwise

ERROR

B.2.2.1.23    DBGCLAIMCLR\_EL1, Debug CLAIM Tag Clear Register

Used by software to read the values of the CLAIM tag bits, and to clear CLAIM tag bits to 0.

The architecture does not define any functionality for the CLAIM tag bits.



CLAIM tags are typically used for communication between the debugger and target software.

Used in conjunction with the ext-DBGCLAIMSET\_EL1 register.

Configurations

An implementation must include eight CLAIM tag bits.

External register DBGCLAIMCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.16 DBGCLAIMCLR\\_EL1, Debug CLAIM Tag Clear Register](#) on page 1108 bits [31:0].

Attributes

Width

32

Component

Debug

Register offset

0xFA4

Access type

RW1C

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-151: EXT\_DBGCLAIMCLR\_EL1 bit assignments

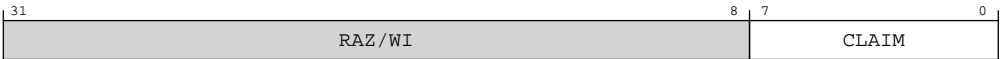


Table B-309: DBGCLAIMCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RAZ/WI	Reserved	RAZ/ WI

Bits	Name	Description	Reset
[7:0]	CLAIM	Read or clear CLAIM tag bits. Reading this field returns the current value of the CLAIM tag bits.  Writing a 1 to one of these bits clears the corresponding CLAIM tag bit to 0. This is an indirect write to the CLAIM tag bits. A single write operation can clear multiple CLAIM tag bits to 0.  Writing 0 to one of these bits has no effect.	0x00

Accessibility

Component	Offset	Instance	Range
Debug	0xFA4	DBGCLAIMCLR_EL1	None

This interface is accessible as follows:

**When IsCorePowered() and !OSLockStatus()**

RW

**Otherwise**

ERROR

B.2.2.1.24 EDDEVAFF0, External Debug Device Affinity register 0

Copy of the low half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the external debug component relates to.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFA8

Access type

See bit descriptions

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-152: EXT\_EDDEVAFF0 bit assignments

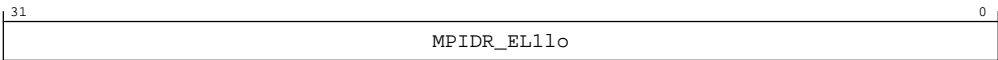


Table B-311: EDDEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1lo	AArch64-MPIDR_EL1 low half. Read-only copy of the low half of AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.	32 {x}

Accessibility

Component	Offset	Instance	Range
Debug	0xFA8	EDDEVAFF0	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.25 EDDEVAFF1, External Debug Device Affinity register 1

Copy of the high half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the external debug component relates to.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug


Register offset

0xFAC

**Access type**  
See bit descriptions

**Reset value**

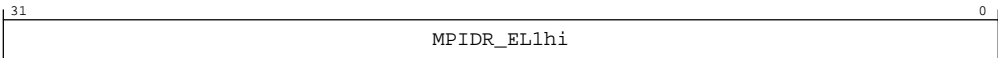


 Where the reset reads xxxx, see individual bits.

Note

**Bit descriptions**

**Figure B-153: EXT\_EDDEVAFF1 bit assignments**



**Table B-313: EDDEVAFF1 bit descriptions**

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1hi	AArch64-MPIDR_EL1 high half. Read-only copy of the high half of AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.	32 {x}

**Accessibility**

Component	Offset	Instance	Range
Debug	0xFAC	EDDEVAFF1	None

This interface is accessible as follows:

**When IsCorePowered()**  
RO

**Otherwise**  
ERROR

**B.2.2.1.26 EDLAR, External Debug Lock Access Register**

Allows or disallows access to the external debug registers through a memory-mapped interface.

The optional Software Lock provides a lock to prevent memory-mapped writes to the debug registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the debug registers. It does not, and cannot, prevent all accidental or malicious damage.



Configurations

Software Lock is not implemented by the architecturally-defined debug components of the PE in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFB0

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Otherwise

Figure B-154: EXT\_EDLAR bit assignments

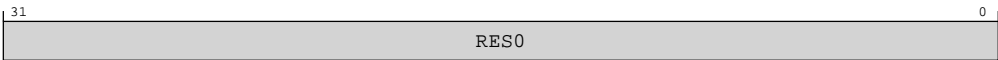


Table B-315: EDLAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
Debug	0xFB0	EDLAR	None

This interface is accessible as follows:

**When IsCorePowered()**

WO

**Otherwise**

ERROR

**B.2.2.1.27 EDLSR, External Debug Lock Status Register**

Indicates the current status of the software lock for external debug registers.

The optional Software Lock provides a lock to prevent memory-mapped writes to the debug registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the debug registers. It does not, and cannot, prevent all accidental or malicious damage.

**Configurations**

Software Lock is not implemented by the architecturally-defined debug components of the PE in the Core power domain.

**Attributes**

**Width**

32

**Component**

Debug

**Register offset**

0xFB4

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx00
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-155: EXT\_EDLSR bit assignments

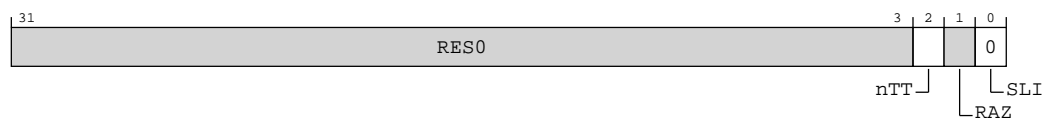


Table B-317: EDLSR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	nTT	Not thirty-two bit access required. <b>RAZ</b> .	x
[1]	RAZ	Reserved	RAZ
[0]	SLI	Indicates whether the Software Lock is implemented.  <b>0b0</b> Software Lock not implemented or not memory-mapped access.	0b0

Accessibility

Component	Offset	Instance	Range
Debug	0xFB4	EDLSR	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.1.28 DBGAUTHSTATUS\_EL1, Debug Authentication Status Register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for debug.

Configurations

This register is in the Core power domain.

External register DBGAUTHSTATUS\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.5.17 DBGAUTHSTATUS\\_EL1, Debug Authentication Status Register](#) on page 1110 bits [31:0].

Attributes

**Width**

32

Component

Debug

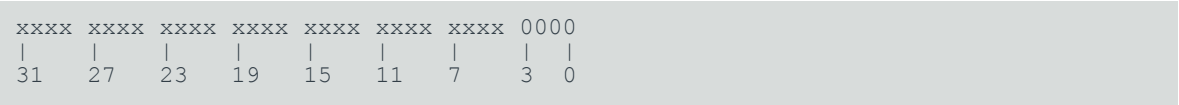
Register offset

0xFB8

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-156: EXT\_DBGAUTHSTATUS\_EL1 bit assignments



Table B-319: DBGAUTHSTATUS\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure non-invasive debug.  This field has the same value as DBGAUTHSTATUS_EL1.SID.	xx
[5:4]	SID	Secure invasive debug.  <b>0b10</b> Implemented and disabled. ExternalSecureInvasiveDebugEnabled() == FALSE.  <b>0b11</b> Implemented and enabled. ExternalSecureInvasiveDebugEnabled() == TRUE.  All other values are reserved.	xx
[3:2]	NSNID	Non-secure non-invasive debug.  <b>0b00</b> Non-secure state is not implemented.  All other values are reserved.	0b00

Bits	Name	Description	Reset
[1:0]	NSID	Non-secure invasive debug.  <b>0b00</b> Non-secure state is not implemented.  All other values are reserved.	0b00

Accessibility

Component	Offset	Instance	Range
Debug	0xFB8	DBGAUTHSTATUS_EL1	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.29 EDDEVARCH, External Debug Device Architecture Register

Identifies the programmers' model architecture of the external debug component.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFBC

Access type

See bit descriptions

Reset value

0100 0111 0111 0000 1001 1010 0000 0101

Bit descriptions

Figure B-157: EXT\_EDDEVARCH bit assignments

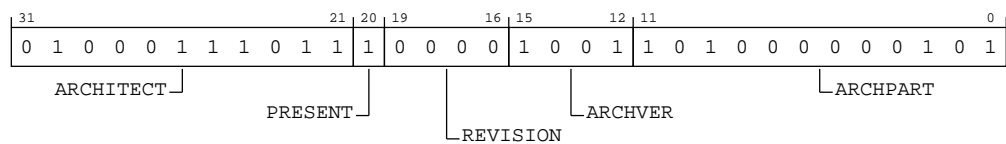


Table B-321: EDDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Defines the architecture of the component. For debug, this is Arm Limited.  Bits [31:28] are the JEP106 continuation code, 0x4.  Bits [27:21] are the JEP106 ID code, 0x3B. <b>0b01000111011</b>	0b01000111011
[20]	PRESENT	Indicates that the DEVARCH is present. <b>0b1</b>	0b1
[19:16]	REVISION	Defines the architecture revision. For architectures defined by Arm this is the minor revision.  For debug, the revision defined by Armv8 is 0x0.  All other values are reserved. <b>0b0000</b>	0b0000
[15:12]	ARCHVER	Architecture Version. Defines the architecture version of the component. Defined values are: <b>0b1001</b> Armv8.4 debug architecture, FEAT_Debugv8p4.	0b1001
[11:0]	ARCHPART	Architecture Part. Defines the architecture of the component. <b>0b101000000101</b> Armv8-R debug architecture.  EDDEVARCH.ARCHVER and EDDEVARCH.ARCHPART are also defined as a single field, EDDEVARCH.ARCHID, so that EDDEVARCH.ARCHPART is EDDEVARCH.ARCHID[11:0].  Armv8-R debug architecture.	0xA05

Accessibility

Component	Offset	Instance	Range
Debug	0xFBC	EDDEVARCH	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise  
ERROR

B.2.2.1.30 EDDEVID2, External Debug Device ID register 2

Reserved for future descriptions of features of the debug implementation.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFC0

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-158: EXT\_EDDEVID2 bit assignments

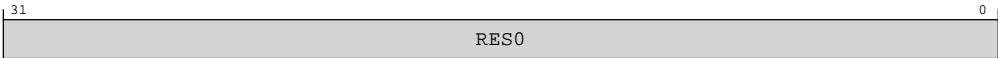


Table B-323: EDDEVID2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
Debug	0xFC0	EDDEVID2	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.31 EDDEVID1, External Debug Device ID Register 1

Provides extra information for external debuggers about features of the debug implementation.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFC4

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure B-159: EXT\_EDDEVID1 bit assignments

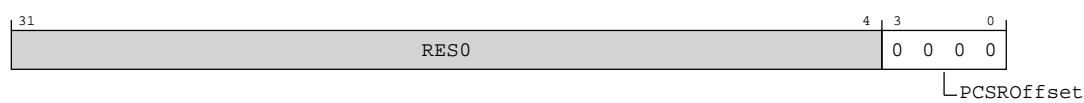


Table B-325: EDDEVID1 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	PCSROffset	Indicates the offset applied to PC samples returned by reads of ext-EDPCSR. Permitted values of this field in Armv8 are:  0b0000 ext-EDPCSR not implemented.	0b0000

Accessibility

Component	Offset	Instance	Range
Debug	0xFC4	EDDEVID1	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.32 EDDEVID, External Debug Device ID register 0

Provides extra information for external debuggers about features of the debug implementation.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFC8

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-160: EXT\_EDDEVID bit assignments

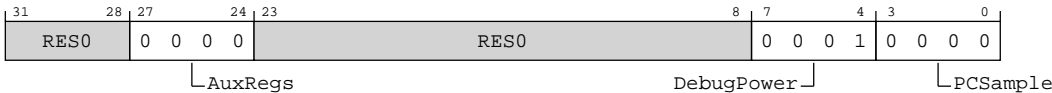


Table B-327: EDDEVID bit descriptions

Bits	Name	Description	Reset
[31:28]	RES0	Reserved	RES0
[27:24]	AuxRegs	Indicates support for Auxiliary registers. Defined values are:  0b0000 None supported.	0b0000
[23:8]	RES0	Reserved	RES0
[7:4]	DebugPower	Indicates support for the FEAT_DoPD feature. Defined values are:  0b0001 FEAT_DoPD implemented. All registers in the external debug interface register map are implemented in the Core power domain.	0b0001
[3:0]	PCSample	Indicates the level of PC Sample-based Profiling support using external debug registers. Defined values are:  0b0000 PC Sample-based Profiling Extension is not implemented in the external debug registers space.	0b0000

Accessibility

Component	Offset	Instance	Range
Debug	0xFC8	EDDEVID	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.33 EDDEVTTYPE, External Debug Device Type register

Indicates to a debugger that this component is part of a PE's debug logic.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFCC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-161: EXT\_EDDEVTTYPE bit assignments



Table B-329: EDDEVTTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Subtype. Indicates this is a component within a PE. 0b0001	0b0001
[3:0]	MAJOR	Major type. Indicates this is a debug logic component. 0b0101	0b0101

Accessibility

Component	Offset	Instance	Range
Debug	0xFCC	EDDEVTYPE	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.34 EDPIDR4, External Debug Peripheral Identification Register 4

Provides information to identify an external debug component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFD0

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-162: EXT\_EDPIDR4 bit assignments



Table B-331: EDPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	Size of the component. <b>RAZ</b> . Log <sub>2</sub> of the number of 4KB pages from the start of the component to the end of the component ID registers.  <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	Designer, JEP106 continuation code, least significant nibble. For Arm Limited, this field is 0b0100.  <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Instance	Range
Debug	0xFD0	EDPIDR4	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.35 EDPIDR0, External Debug Peripheral Identification Register 0

Provides information to identify an external debug component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFE0

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-163: EXT\_EDPIDR0 bit assignments

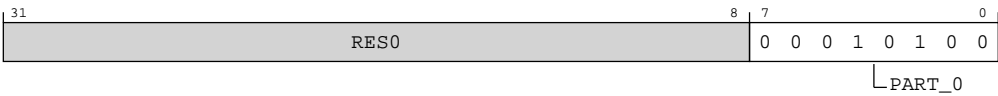


Table B-333: EDPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b00010100 Cortex-R82AE external debug. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Instance	Range
Debug	0xFE0	EDPIDR0	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.36    EDPIDR1, External Debug Peripheral Identification Register 1

Provides information to identify an external debug component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFE4

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-164: EXT\_EDPIDR1 bit assignments

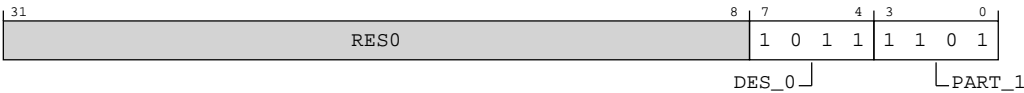


Table B-335: EDPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	Designer, least significant nibble of JEP106 ID code. For Arm Limited, this field is 0b1011.  0b1011 Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011

Bits	Name	Description	Reset
[3:0]	PART_1	Part number bits [11:8].  <b>0b1101</b> Cortex-R82AE external debug. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Instance	Range
Debug	0xFE4	EDPIDR1	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.37    EDPIDR2, External Debug Peripheral Identification Register 2

Provides information to identify an external debug component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFE8

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0111	1011
31	27	23	19	15	11	7	3 0





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-165: EXT\_EDPIDR2 bit assignments

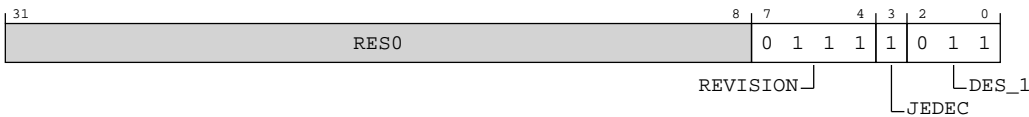


Table B-337: EDPIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Instance	Range
Debug	0xFE8	EDPIDR2	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.38 EDPIDR3, External Debug Peripheral Identification Register 3

Provides information to identify an external debug component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFEC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-166: EXT\_EDPIDR3 bit assignments

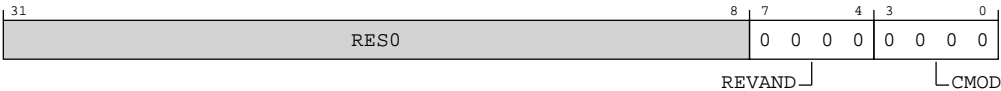


Table B-339: EDPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Part minor revision. Parts using ext-EDPIDR2.REVISION as an extension to the Part number must use this field as a major revision number.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer modified. Indicates someone other than the Designer has modified the component.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Instance	Range
Debug	0xFEC	EDPIDR3	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.39 EDCIDR0, External Debug Component Identification Register 0

Provides information to identify an external debug component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFF0

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	1101
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-167: EXT\_EDCIDR0 bit assignments

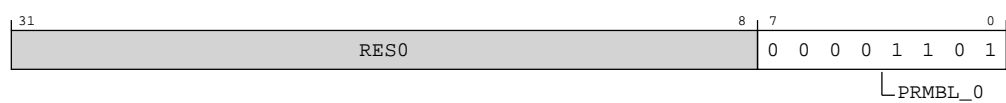


Table B-341: EDCIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble. <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Instance	Range
Debug	0xFF0	EDCIDR0	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.40 EDCIDR1, External Debug Component Identification Register 1

Provides information to identify an external debug component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

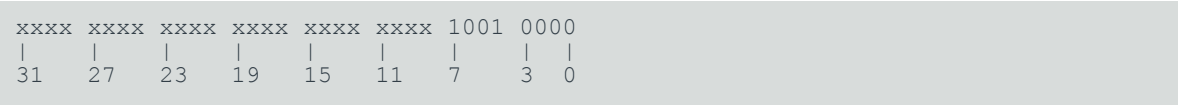
Register offset

0xFF4

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-168: EXT\_EDCIDR1 bit assignments



Table B-343: EDCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	Component class. <b>0b1001</b> CoreSight debug component.	0b1001
[3:0]	PRMBL_1	Preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Instance	Range
Debug	0xFF4	EDCIDR1	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.41 EDCIDR2, External Debug Component Identification Register 2

Provides information to identify an external debug component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFF8

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-169: EXT\_EDCIDR2 bit assignments

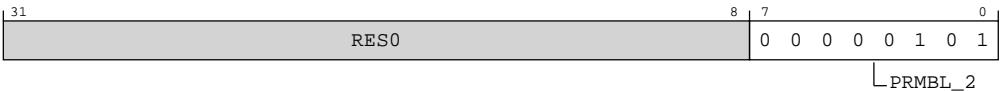


Table B-345: EDCIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble.  0b000000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Instance	Range
Debug	0xFF8	EDCIDR2	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.1.42 EDCIDR3, External Debug Component Identification Register 3

Provides information to identify an external debug component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

Debug

Register offset

0xFFC

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0001
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-170: EXT\_EDCIDR3 bit assignments



Table B-347: EDCIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble. <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Instance	Range
Debug	0xFFC	EDCIDR3	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2 External CLUSTERPMU register description

This section includes the register descriptions for all memory-mapped CLUSTERPMU registers that are accessed for the cluster.

B.2.2.2.1 CLUSTERPMU\_PMEVCNTR<n>\_EL1, Cluster Performance Monitors Event Count Registers, n = 0 - 5

Holds event counter n, which counts events, where n is 0 to 30.

Configurations

This register is available in all configurations.

Attributes

Width

32




**Component**  
CLUSTERPMU

**Register offset**  
0x000 + (8 \* n)

**Access type**  
See bit descriptions

**Reset value**

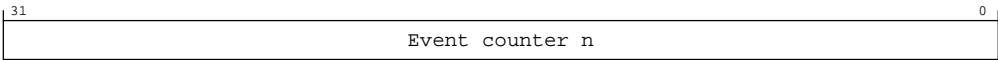


 Where the reset reads xxxx, see individual bits.

Note

**Bit descriptions**

**Figure B-171: EXT\_CLUSTERPMU\_PMEVCNTR<n>\_EL1 bit assignments**



**Table B-349: CLUSTERPMU\_PMEVCNTR<n>\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31:0]	None	Event counter n. Value of event counter n, where n is the number of this register and is a number from 0 to 30.	32 {x}

**Accessibility**

Component	Offset	Range
CLUSTERPMU	0x000 + (8 * n)	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
RW

**Otherwise**  
ERROR

B.2.2.2.2 CLUSTERPMU\_PMCCNTR\_EL1, Cluster Performance Monitors Cycle Counter

Holds the value of the Cluster Cycle Counter, CCNT, that counts processor clock cycles.

Configurations

External register CLUSTERPMU\_PMCCNTR\_EL1 bits [63:0] are architecturally mapped to AArch64 System register [A.2.3.12 IMP\\_CLUSTERPMCCNTR\\_EL1, Cluster Performance Monitors Cycle Count Register](#) on page 777 bits [63:0].

Attributes

Width

64

Component

CLUSTERPMU

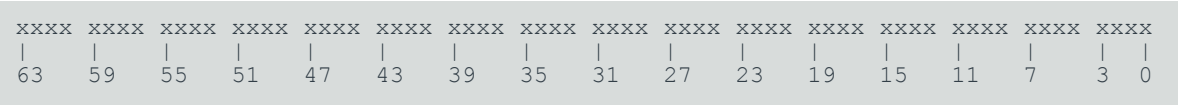
Register offsets (2)

0x0F8,0x0FC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-172: EXT\_CLUSTERPMU\_PMCCNTR\_EL1 bit assignments

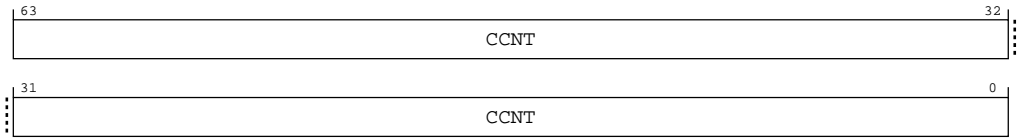


Table B-351: CLUSTERPMU\_PMCCNTR\_EL1 bit descriptions

Bits	Name	Description	Reset
[63:0]	CCNT	Cycle count. The cycle count increments in every processor clock cycle.  Writing 1 to ext-CLUSTERPMU_PMCRR_EL1.C sets this field to 0.	64 {x}

Accessibility

Component	Offset	Range
CLUSTERPMU	0x0F8	31:0

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
RW

**Otherwise**  
ERROR

Component	Offset	Range
CLUSTERPMU	0x0FC	63:32

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
RW

**Otherwise**  
ERROR

B.2.2.2.3 CLUSTERPMU\_PMEVTYPEPER<n>\_EL1, Cluster Performance Monitors Event Type Registers, n = 0 - 5

Configures event counter n, where n is 0 to 30.

Configurations

If event counter n is not implemented then accesses to this register are RES0.

Attributes

**Width**  
32

**Component**  
CLUSTERPMU

**Register offset**  
 $0x400 + (4 * n)$

**Access type**  
See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-173: EXT\_CLUSTERPMU\_PMEVTYPEPER<n>\_EL1 bit assignments

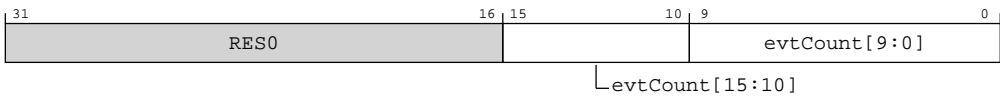


Table B-354: CLUSTERPMU\_PMEVTYPEPER<n>\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0
[15:10]	evtCount[15:10]	Extension to evtCount[9:0]. See evtCount[9:0] for more details.	6 {x}
[9:0]	evtCount[9:0]	<p>Event to count. The event number of the event that is counted by event counter ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>Software must program this field with an event that is supported by the PE being programmed.</p> <p>There are three types of event:</p> <ul style="list-style-type: none"><li>Common architectural and microarchitectural events.</li><li>Arm recommended common architectural and microarchitectural events.</li><li>IMPLEMENTATION DEFINED events.</li></ul> <p>The ranges of event numbers allocated to each type of event are shown in .</p> <p>If evtCount is programmed to an event that is reserved or not supported by the PE, the behavior depends on the event type:</p> <ul style="list-style-type: none"><li>For the range 0x000 to 0x03F, no events are counted, and the value returned by a direct or external read of the evtCount field is the value written to the field.</li><li>For IMPLEMENTATION DEFINED events, it is UNPREDICTABLE what event, if any, is counted, and the value returned by a direct or external read of the evtCount field is <b>UNKNOWN</b>.</li></ul> <p><b>Note:</b> UNPREDICTABLE means the event must not expose privileged information.</p> <p>Arm recommends that the behavior across a family of implementations is defined such that if a given implementation does not include an event from a set of common IMPLEMENTATION DEFINED events, then no event is counted and the value read back on evtCount is the value written.</p>	10 {x}

Accessibility

Component	Offset	Range
CLUSTERPMU	0x400 + (4 * n)	None

This interface is accessible as follows:

When IsCorePowered() and AllowExternalPMUAccess()

RW

Otherwise

ERROR

B.2.2.2.4 CLUSTERPMU\_PMCCFILTR\_EL1, Cluster Performance Monitors Cycle Counter Filter Register

Determines the modes in which the Cluster Cycle Counter, ext-CLUSTERPMU\_PMCCNTR\_EL1, increments. Unlike the per-core PMUs, the Cluster Cycle Counter always increments.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0x47C

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-174: EXT\_CLUSTERPMU\_PMCCFILTR\_EL1 bit assignments

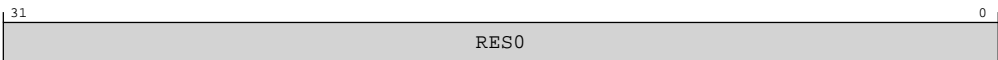


Table B-356: CLUSTERPMU\_PMCCFILTR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERPMU	0x47C	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RW

**Otherwise**

ERROR

B.2.2.2.5 CLUSTERPMU\_PMCNTENSET\_EL1, Cluster Performance Monitors Count Enable Set register

Enables the Cycle Count Register, ext-CLUSTERPMU\_PMCCNTR\_EL1, and any implemented event counters AArch64-IMP\_CLUSTERPMEVCNTR<n>. Reading this register shows which counters are enabled.

Configurations

External register CLUSTERPMU\_PMCNTENSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register A.2.3.5 IMP\_CLUSTERPMCNTENSET\_EL1, Cluster Performance Monitors Count Enable Set register on page 762 bits [31:0].

Attributes

**Width**

32

**Component**

CLUSTERPMU

**Register offset**

0xC00

**Access type**

RW1S

**Reset value**

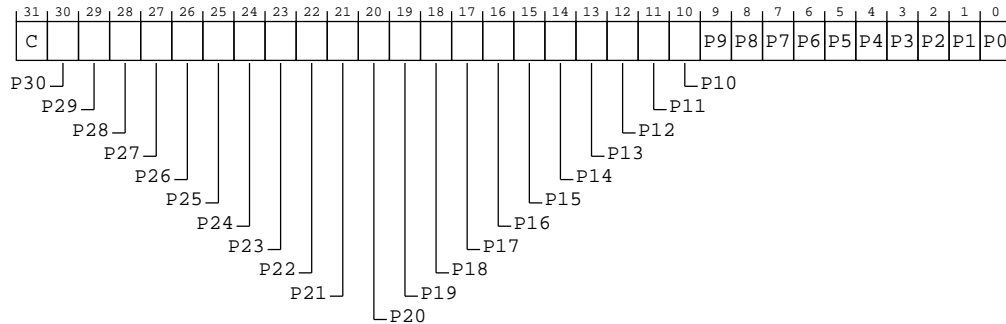


**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-175: EXT\_CLUSTERPMU\_PMCNTENSET\_EL1 bit assignments**



**Table B-358: CLUSTERPMU\_PMCNTENSET\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31]	C	ext-CLUSTERPMU_PMCCNTR_EL1 enable bit. Enables the cycle counter register. Possible values are:  <b>0b0</b> When read, means the cycle counter is disabled. When written, has no effect.  <b>0b1</b> When read, means the cycle counter is enabled. When written, enables the cycle counter.	x
[30:0]	P<n>, bit[n], where n = 30 to 0	Event counter enable bit for ext-CLUSTERPMU_PMEVCNTR<n>_EL1.  If ext-CLUSTERPMU_PMCFGR.N is less than 31, bits [30:ext-CLUSTERPMU_PMCFGR.N] are <b>RAZ/WI</b> .  <b>0b0</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is disabled. When written, has no effect.  <b>0b1</b> When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 event counter is enabled. When written, enables ext-CLUSTERPMU_PMEVCNTR<n>_EL1.	31 {x}

## Accessibility

Component	Offset	Range
CLUSTERPMU	0xC00	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RW

Otherwise  
ERROR

B.2.2.2.6 CLUSTERPMU\_PMCNTENCLR\_EL1, Cluster Performance Monitors Count Enable Clear register

Disables the Cycle Count Register, ext-CLUSTERPMU\_PMCCNTR\_EL1, and any implemented event counters AArch64-IMP\_CLUSTERPMEVCNTR<n>. Reading this register shows which counters are enabled.

Configurations

External register CLUSTERPMU\_PMCNTENCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.6 IMP\\_CLUSTERPMCNTENCLR\\_EL1, Cluster Performance Monitors Count Enable Clear register](#) on page 764 bits [31:0].

Attributes

Width  
32

Component  
CLUSTERPMU

Register offset  
0xC20

Access type  
RW1C

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure B-176: EXT\_CLUSTERPMU\_PMCNTENCLR\_EL1 bit assignments

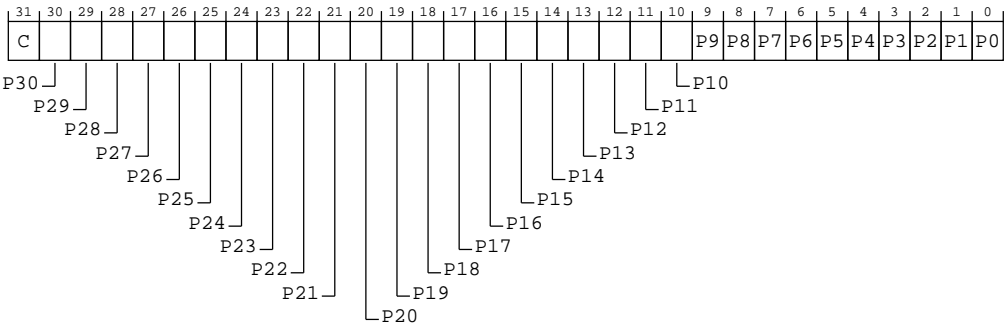


Table B-360: CLUSTERPMU\_PMCNTENCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31]	C	ext-CLUSTERPMU_PMCNTR_EL1 disable bit. Disables the cycle counter register. Possible values are:  <b>0b0</b>  When read, means the cycle counter is disabled. When written, has no effect.  <b>0b1</b>  When read, means the cycle counter is enabled. When written, disables the cycle counter.	x
[30:0]	P<n>, bit[n], where n = 30 to 0	Event counter disable bit for ext-CLUSTERPMU_PMEVCNTR<n>_EL1.  If ext-CLUSTERPMU_PMCFGR.N is less than 31, bits [30:ext-CLUSTERPMU_PMCFGR.N] are <b>RAZ/WI</b> .  <b>0b0</b>  When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is disabled. When written, has no effect.  <b>0b1</b>  When read, means that ext-CLUSTERPMU_PMEVCNTR<n>_EL1 is enabled. When written, disables ext-CLUSTERPMU_PMEVCNTR<n>_EL1.	31 {x}

Accessibility

Component	Offset	Range
CLUSTERPMU	0xC20	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
RW

**Otherwise**  
ERROR

### B.2.2.2.7 CLUSTERPMU\_PMINTENSET\_EL1, Cluster Performance Monitors Interrupt Enable Set register

Enables the generation of interrupt requests on overflows from the Cycle Count Register, ext-CLUSTERPMU\_PMCNTR\_EL1, and the event counters ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1. Reading the register shows which overflow interrupt requests are enabled.

#### Configurations

External register CLUSTERPMU\_PMINTENSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.10 IMP\\_CLUSTERPMINTENSET\\_EL1, Cluster Performance Monitors Interrupt Enable Set register](#) on page 773 bits [31:0].

#### Attributes

##### Width

32

##### Component

CLUSTERPMU

##### Register offset

0xC40

##### Access type

RW1S

##### Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0

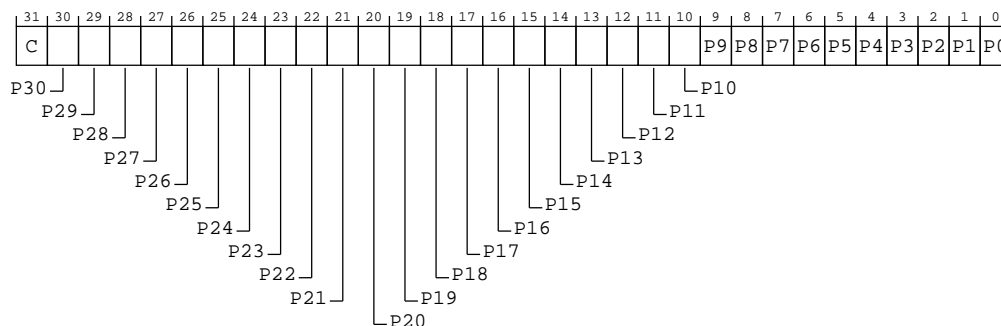


Note

Where the reset reads xxxx, see individual bits.

#### Bit descriptions

Figure B-177: EXT\_CLUSTERPMU\_PMINTENSET\_EL1 bit assignments



**Table B-362: CLUSTERPMU\_PMINTENSET\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31]	C	<p>ext-CLUSTERPMU_PMCNTR_EL1 overflow interrupt request enable bit. Possible values are:</p> <p><b>0b0</b></p> <p>When read, means the cycle counter overflow interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter overflow interrupt request is enabled. When written, enables the cycle count overflow interrupt request.</p>	x
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow interrupt request enable bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>If ext-CLUSTERPMU_PMCNTR.N is less than 31, bits [30:ext-CLUSTERPMU_PMCNTR.N] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is enabled. When written, enables the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 interrupt request.</p>	31 {x}

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xC40	None

This interface is accessible as follows:

#### When IsCorePowered() and AllowExternalPMUAccess()

RW

#### Otherwise

ERROR

#### B.2.2.2.8 CLUSTERPMU\_PMINTENCLR\_EL1, Cluster Performance Monitors Interrupt Enable Clear register

Disables the generation of interrupt requests on overflows from the Cycle Count Register, ext-CLUSTERPMU\_PMCNTR\_EL1, and the event counters ext-CLUSTERPMU\_PMEVCNTR<n>\_EL1. Reading the register shows which overflow interrupt requests are enabled.

### Configurations

External register CLUSTERPMU\_PMINTENCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.11 IMP\\_CLUSTERPMINTENCLR\\_EL1, Cluster Performance Monitors Interrupt Enable Clear register](#) on page 775 bits [31:0].

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xC60

Access type

RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-178: EXT\_CLUSTERPMU\_PMINTENCLR\_EL1 bit assignments

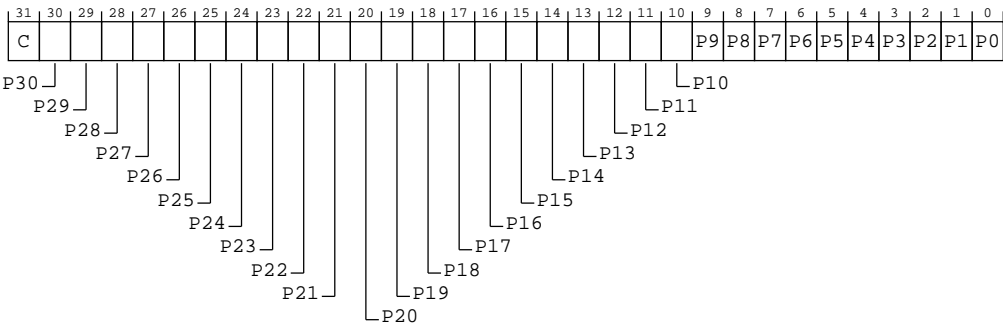


Table B-364: CLUSTERPMU\_PMINTENCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31]	C	<div>ext-CLUSTERPMU_PMCCNTR_EL1 overflow interrupt request disable bit. Possible values are:</div> <div><b>0b0</b></div> <div>When read, means the cycle counter overflow interrupt request is disabled. When written, has no effect.</div> <div><b>0b1</b></div> <div>When read, means the cycle counter overflow interrupt request is enabled. When written, disables the cycle count overflow interrupt request.</div>	x

Bits	Name	Description	Reset
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow interrupt request disable bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1.</p> <p>If ext-CLUSTERPMU_PMCFCGR.N is less than 31, bits [30:ext-CLUSTERPMU_PMCFCGR.N] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is disabled. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 event counter interrupt request is enabled. When written, disables the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 interrupt request.</p>	31 {x}

## Accessibility

Component	Offset	Range
CLUSTERPMU	0xC60	None

This interface is accessible as follows:

### When IsCorePowered() and AllowExternalPMUAccess()

RW

### Otherwise

ERROR

#### B.2.2.2.9 CLUSTERPMU\_PMOVSLR\_EL1, Cluster Performance Monitors Overflow Flag Status Clear register

Contains the state of the overflow bit for the Cycle Count Register, ext-CLUSTERPMU\_PMCNTR\_EL1, and each of the implemented event counters AArch32-PMEVCNTR<n>. Writing to this register clears these bits.

## Configurations

External register CLUSTERPMU\_PMOVSLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.8 IMP\\_CLUSTERPMOVSLR\\_EL1, Cluster Performance Monitors Overflow Flag Status Clear Register](#) on page 768 bits [31:0].

## Attributes

### Width

32

### Component

CLUSTERPMU

### Register offset

0xC80

### Access type

RW1C

## Reset value

```

xxxx  xxxx  xxxx  xxxx  xxxx  xxxx  xxxx  xxxx
|      |      |      |      |      |      |      |
31     27     23     19     15     11     7       3       0

```



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-179: EXT\_CLUSTERPMU\_PMOVSLR\_EL1 bit assignments

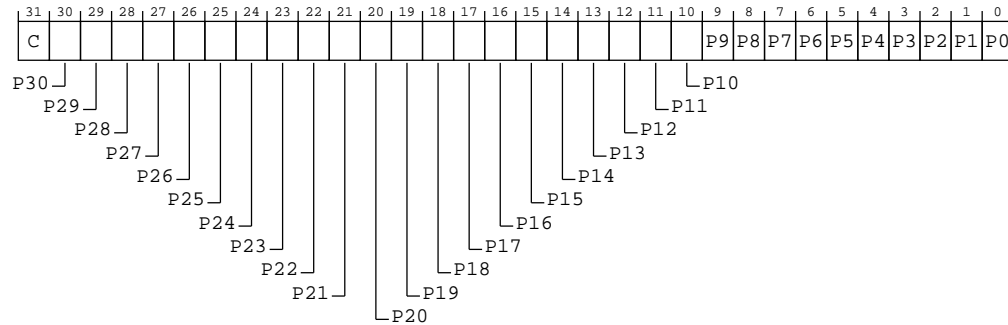


Table B-366: CLUSTERPMU\_PMOVSLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31]	C	<p>Cycle counter overflow clear bit.</p> <p><b>0b0</b></p> <p>When read, means the cycle counter has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter has overflowed since this bit was last cleared. When written, clears the cycle counter overflow bit to 0.</p>	x
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow clear bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1. Bits [30:ext-CLUSTERPMU_PMCFCGR.N] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has overflowed since this bit was last cleared. When written, clears the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 overflow bit to 0.</p>	31 {x}

Accessibility

Component	Offset	Range
CLUSTERPMU	0xC80	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
RW

**Otherwise**  
ERROR

B.2.2.2.10 CLUSTERPMU\_PMSWINC\_EL1, Cluster Performance Monitors Software Increment register

No Software increment events implemented by the Cluster PMU.

Configurations

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMSWINC\_EL1". Otherwise, direct accesses to CLUSTERPMU\_PMSWINC\_EL1 are UNDEFINED.

Attributes

**Width**  
32

**Component**  
CLUSTERPMU

**Register offset**  
0xCA0

**Access type**  
See bit descriptions

**Reset value**  
0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-180: EXT\_CLUSTERPMU\_PMSWINC\_EL1 bit assignments

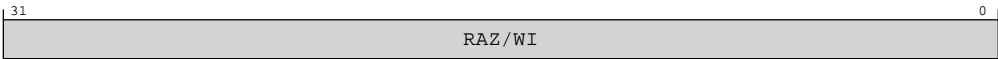


Table B-368: CLUSTERPMU\_PMSWINC\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERPMU	0xCA0	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**  
WO

**Otherwise**  
ERROR

B.2.2.2.11 CLUSTERPMU\_PMOVSET\_EL1, Cluster Performance Monitors Overflow Flag Status Set register

Sets the state of the overflow bit for the Cycle Count Register, ext-CLUSTERPMU\_PMCNTR\_EL1, and each of the implemented event counters AArch32-PMEVCNTR<n>.

Configurations

External register CLUSTERPMU\_PMOVSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register A.2.3.7 IMP\_CLUSTERPMOVSET\_EL1, Cluster Performance Monitors Overflow Flag Status Set register on page 766 bits [31:0].

Attributes

**Width**  
32

**Component**  
CLUSTERPMU

**Register offset**  
0xCC0

**Access type**  
RW1S

**Reset value**



Where the reset reads xxxx, see individual bits.



## Bit descriptions

Figure B-181: EXT\_CLUSTERPMU\_PMOVSET\_EL1 bit assignments

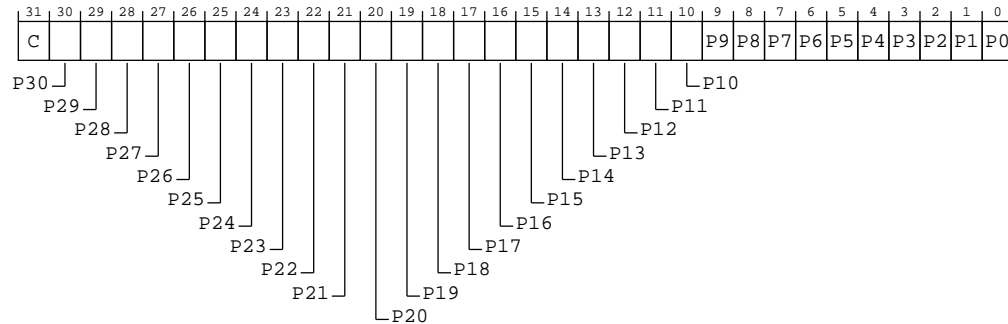


Table B-370: CLUSTERPMU\_PMOVSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[31]	C	<p>Cycle counter overflow set bit.</p> <p><b>0b0</b></p> <p>When read, means the cycle counter has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means the cycle counter has overflowed since this bit was last cleared. When written, sets the cycle counter overflow bit to 1.</p>	x
[30:0]	P<n>, bit[n], where n = 30 to 0	<p>Event counter overflow set bit for ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1. Bits [30:ext-CLUSTERPMU_PMCFCGR.N] are <b>RAZ/WI</b>.</p> <p><b>0b0</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has not overflowed since this bit was last cleared. When written, has no effect.</p> <p><b>0b1</b></p> <p>When read, means that ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 has overflowed since this bit was last cleared. When written, sets the ext-CLUSTERPMU_PMEVCNTR&lt;n&gt;_EL1 overflow bit to 1.</p>	31 {x}

## Accessibility

Component	Offset	Range
CLUSTERPMU	0xCC0	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RW

**Otherwise**

ERROR

B.2.2.2.12 CLUSTERPMU\_PMCFG, Cluster Performance Monitors Configuration Register

Contains PMU-specific configuration data.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

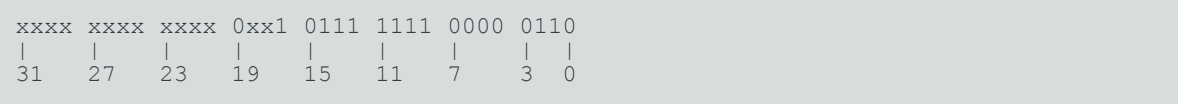
Register offset

0xE00

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-182: EXT\_CLUSTERPMU\_PMCFG bit assignments

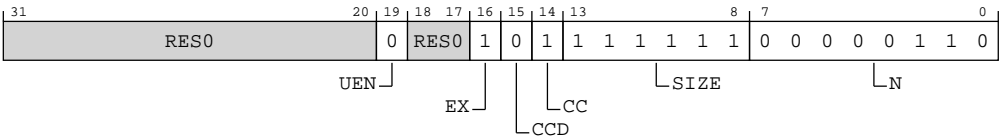


Table B-372: CLUSTERPMU\_PMCFG bit descriptions

Bits	Name	Description	Reset
[31:20]	RES0	Reserved	RES0
[19]	UEN	User-mode Enable Register supported.  0b0 User-mode Enable Register not supported.	0b0
[18:17]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[16]	EX	Export supported. <b>0b1</b> ext-CLUSTERPMU_PMCR_EL1.X is read/write.	0b1
[15]	CCD	Cycle counter has prescale. <b>0b0</b> ext-CLUSTERPMU_PMCR_EL1.D is <b>RES0</b> .	0b0
[14]	CC	Dedicated cycle counter. <b>0b1</b> Dedicated cycle counter ext-CLUSTERPMU_PMCNTR_EL1 is supported.	0b1
[13:8]	SIZE	Size of counters, minus one. This field defines the size of the largest counter implemented by the Performance Monitors Unit.  This field is used by software to determine the spacing of the counters in the memory-map. <b>0b111111</b> The largest counter is 64-bits. Counters are at doubleword-aligned addresses.	0b111111
[7:0]	N	Number of counters implemented in addition to the cycle counter, ext-CLUSTERPMU_PMCNTR_EL1. <b>0b00000110</b> ext-CLUSTERPMU_PMCNTR_EL1 plus six event counters implemented.	0x06

## Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

## Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Range
CLUSTERPMU	0xE00	None

This interface is accessible as follows:

### When IsCorePowered() and AllowExternalPMUAccess()

RO

### Otherwise

ERROR

B.2.2.2.13 CLUSTERPMU\_PMCR\_EL1, Cluster Performance Monitors Control Register

Provides details of the Performance Monitors implementation, including the number of counters implemented, and configures and controls the counters.

Configurations

This register is only partially mapped to the internal AArch64-IMP\_CLUSTERPMCR System register. An external agent must use other means to discover the information held in AArch64-IMP\_CLUSTERPMCR[31:11], such as accessing ext-CLUSTERPMU\_PMCFCGR and the ID registers.

External register CLUSTERPMU\_PMCR\_EL1 bits [7:0] are architecturally mapped to AArch64 System register [A.2.3.4 IMP\\_CLUSTERPMCR\\_EL1, Cluster Performance Monitors Control Register](#) on page 759 bits [7:0].

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xE04

Access type

inconsistent

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000
31	27	23	19	15	11	7	3 0

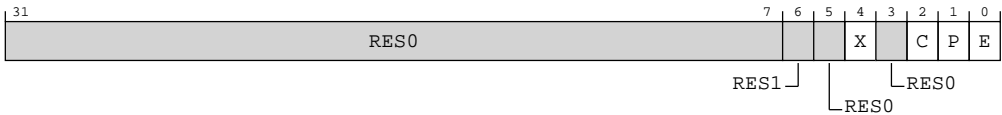


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-183: EXT\_CLUSTERPMU\_PMCR\_EL1 bit assignments



**Table B-374: CLUSTERPMU\_PMCR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31:7]	RES0	Reserved	RES0
[6]	RES1	Reserved	RES1
[5]	RES0	Reserved	RES0
[4]	X	This field enables the exporting of events over an event bus to another device.  <b>0b0</b> Cluster PMU events are not exported externally.	x
[3]	RES0	Reserved	RES0
[2]	C	Cycle counter reset. This bit is WO. The effects of writing to this bit are:  <b>0b0</b> No action.  <b>0b1</b> Reset ext-CLUSTERPMU_PMCNTR_EL1 to zero.  This bit is always <b>RAZ</b> .  <b>Note:</b> Resetting ext-CLUSTERPMU_PMCNTR_EL1 does not change the cycle counter overflow bit.	0b0
[1]	P	Event counter reset. This bit is WO. The effects of writing to this bit are:  <b>0b0</b> No action.  <b>0b1</b> Reset all event counters, not including ext-CLUSTERPMU_PMCNTR_EL1, to zero.  This bit is always <b>RAZ</b> .  <b>Note:</b> Resetting the event counters does not change the event counter overflow bits.	0b0
[0]	E	Enable.  <b>0b0</b> All event counters, including ext-CLUSTERPMU_PMCNTR_EL1, are disabled.  <b>0b1</b> All event counters can be enabled by ext-CLUSTERPMU_PMCNTENSET_EL1.  This bit is RW.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xE04	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RW

**Otherwise**

ERROR

**B.2.2.2.14 CLUSTERPMU\_PMCEID0, Cluster Performance Monitors Common Event Identification register 0**

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the range 0x0000 to 0x001F

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

**Configurations**

External register CLUSTERPMU\_PMCEID0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.15 IMP\\_CLUSTERPMCEID0\\_EL1, Cluster Performance Monitors Common Event Identification register 0](#) on page 783 bits [31:0].

**Attributes**

**Width**

32

**Component**

CLUSTERPMU

**Register offset**

0xE20

**Access type**

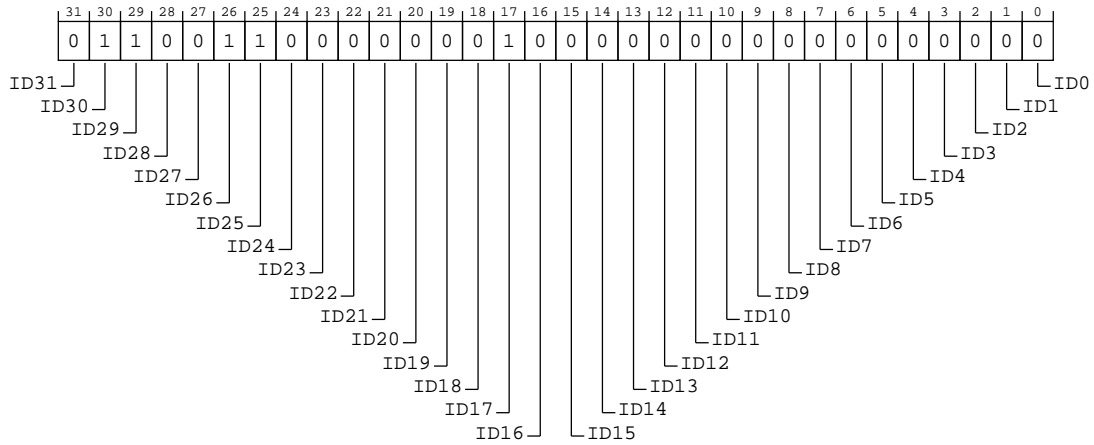
See bit descriptions

**Reset value**

0110 0110 0000 0010 0000 0000 0000 0000

## Bit descriptions

### Figure B-184: EXT\_CLUSTERPMU\_PMCEID0 bit assignments



### Table B-376: CLUSTERPMU\_PMCEID0 bit descriptions

Bits	Name	Description	Reset
[31]	ID31	Common event 0x001F implemented. <b>0b0</b> Event 0x001F not implemented.	0b0
[30]	ID30	Common event 0x001E implemented. <b>0b1</b> CHAIN event implemented.	0b1
[29]	ID29	Common event 0x001D implemented. <b>0b1</b> BUS_CYCLES event implemented.	0b1
[28]	ID28	Common event 0x001C implemented. <b>0b0</b> Event 0x001C not implemented.	0b0
[27]	ID27	Common event 0x001B implemented. <b>0b0</b> Event 0x001B not implemented.	0b0
[26]	ID26	Common event 0x001A implemented. <b>0b1</b> MEMORY_ERROR event implemented.	0b1
[25]	ID25	Common event 0x0019 implemented. <b>0b1</b> BUS_ACCESS event implemented.	0b1
[24]	ID24	Common event 0x0018 implemented. <b>0b0</b> Event 0x0018 not implemented.	0b0

Bits	Name	Description	Reset
[23]	ID23	Common event 0x0017 implemented. <b>0b0</b> Event 0x0017 not implemented.	0b0
[22]	ID22	Common event 0x0016 implemented. <b>0b0</b> Event 0x0016 not implemented.	0b0
[21]	ID21	Common event 0x0015 implemented. <b>0b0</b> Event 0x0015 not implemented.	0b0
[20]	ID20	Common event 0x0014 implemented. <b>0b0</b> Event 0x0014 not implemented.	0b0
[19]	ID19	Common event 0x0013 implemented. <b>0b0</b> Event 0x0013 not implemented.	0b0
[18]	ID18	Common event 0x0012 implemented. <b>0b0</b> Event 0x0012 not implemented.	0b0
[17]	ID17	Common event 0x0011 implemented. <b>0b1</b> CYCLES event implemented.	0b1
[16]	ID16	Common event 0x0010 implemented. <b>0b0</b> Event 0x0010 not implemented.	0b0
[15]	ID15	Common event 0x000F implemented. <b>0b0</b> Event 0x000F not implemented.	0b0
[14]	ID14	Common event 0x000E implemented. <b>0b0</b> Event 0x000E not implemented.	0b0
[13]	ID13	Common event 0x000D implemented. <b>0b0</b> Event 0x000D not implemented.	0b0
[12]	ID12	Common event 0x000C implemented. <b>0b0</b> Event 0x000C not implemented.	0b0
[11]	ID11	Common event 0x000B implemented. <b>0b0</b> Event 0x000B not implemented.	0b0
[10]	ID10	Common event 0x000A implemented. <b>0b0</b> Event 0x000A not implemented.	0b0



Bits	Name	Description	Reset
[9]	ID9	Common event 0x0009 implemented. <b>0b0</b> Event 0x0009 not implemented.	0b0
[8]	ID8	Common event 0x0008 implemented. <b>0b0</b> Event 0x0008 not implemented.	0b0
[7]	ID7	Common event 0x0007 implemented. <b>0b0</b> Event 0x0007 not implemented.	0b0
[6]	ID6	Common event 0x0006 implemented. <b>0b0</b> Event 0x0006 not implemented.	0b0
[5]	ID5	Common event 0x0005 implemented. <b>0b0</b> Event 0x0005 not implemented.	0b0
[4]	ID4	Common event 0x0004 implemented. <b>0b0</b> Event 0x0004 not implemented.	0b0
[3]	ID3	Common event 0x0003 implemented. <b>0b0</b> Event 0x0003 not implemented.	0b0
[2]	ID2	Common event 0x0002 implemented. <b>0b0</b> Event 0x0002 not implemented.	0b0
[1]	ID1	Common event 0x0001 implemented. <b>0b0</b> Event 0x0001 not implemented.	0b0
[0]	ID0	Common event 0x0000 implemented. <b>0b0</b> Event 0x0000 not implemented.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xE20	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RO

**Otherwise**

ERROR

### B.2.2.2.15 CLUSTERPMU\_PMCEID1, Cluster Performance Monitors Common Event Identification register 1

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the range 0x020 to 0x03F.

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

#### Configurations

External register CLUSTERPMU\_PMCEID1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.16 IMP\\_CLUSTERPMCEID1\\_EL1, Cluster Performance Monitors Common Event Identification register 1](#) on page 790 bits [31:0].

#### Attributes

##### Width

32

##### Component

CLUSTERPMU

##### Register offset

0xE24

##### Access type

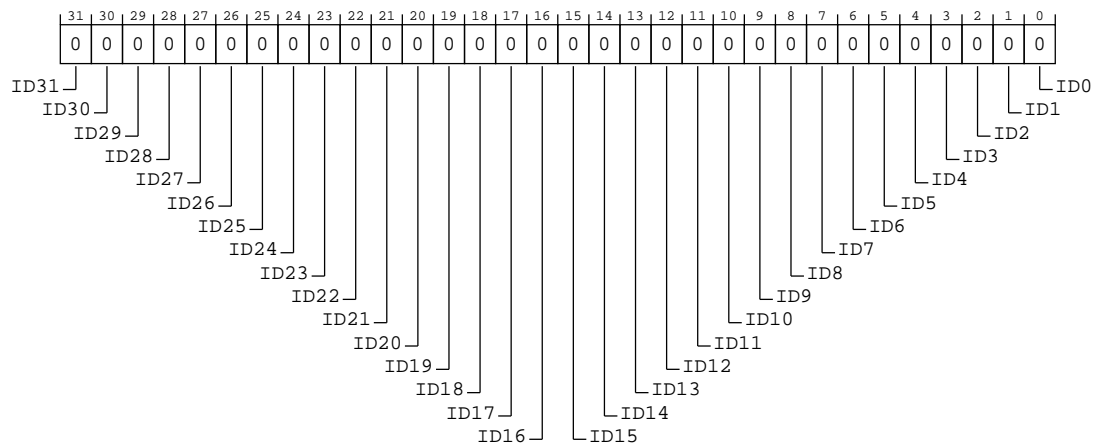
See bit descriptions

##### Reset value

0000 0000 0000 0000 0000 0000 0000 0000

#### Bit descriptions

**Figure B-185: EXT\_CLUSTERPMU\_PMCEID1 bit assignments**



**Table B-378: CLUSTERPMU\_PMCEID1 bit descriptions**

Bits	Name	Description	Reset
[31]	ID31	Common event 0x003F implemented. <b>0b0</b> Event 0x003F not implemented.	0b0
[30]	ID30	Common event 0x003E implemented. <b>0b0</b> Event 0x003E not implemented.	0b0
[29]	ID29	Common event 0x003D implemented. <b>0b0</b> Event 0x003D not implemented.	0b0
[28]	ID28	Common event 0x003C implemented. <b>0b0</b> Event 0x003C not implemented.	0b0
[27]	ID27	Common event 0x003B implemented. <b>0b0</b> Event 0x003B not implemented.	0b0
[26]	ID26	Common event 0x003A implemented. <b>0b0</b> Event 0x003A not implemented.	0b0
[25]	ID25	Common event 0x0039 implemented. <b>0b0</b> Event 0x0039 not implemented.	0b0
[24]	ID24	Common event 0x0038 implemented. <b>0b0</b> Event 0x0038 not implemented.	0b0
[23]	ID23	Common event 0x0037 implemented. <b>0b0</b> Event 0x0037 not implemented.	0b0
[22]	ID22	Common event 0x0036 implemented. <b>0b0</b> Event 0x0036 not implemented.	0b0
[21]	ID21	Common event 0x0035 implemented. <b>0b0</b> Event 0x0035 not implemented.	0b0
[20]	ID20	Common event 0x0034 implemented. <b>0b0</b> Event 0x0034 not implemented.	0b0
[19]	ID19	Common event 0x0033 implemented. <b>0b0</b> Event 0x0033 not implemented.	0b0

Bits	Name	Description	Reset
[18]	ID18	Common event 0x0032 implemented. <b>0b0</b> Event 0x0032 not implemented.	0b0
[17]	ID17	Common event 0x0031 implemented. <b>0b0</b> Event 0x0031 not implemented.	0b0
[16]	ID16	Common event 0x0030 implemented. <b>0b0</b> Event 0x0030 not implemented.	0b0
[15]	ID15	Common event 0x002F implemented. <b>0b0</b> Event 0x002F not implemented.	0b0
[14]	ID14	Common event 0x002E implemented. <b>0b0</b> Event 0x002E not implemented.	0b0
[13]	ID13	Common event 0x002D implemented. <b>0b0</b> Event 0x002D not implemented.	0b0
[12]	ID12	Common event 0x002C implemented. <b>0b0</b> Event 0x002C not implemented.	0b0
[11]	ID11	Common event 0x002B implemented. <b>0b0</b> Event 0x002B not implemented.	0b0
[10]	ID10	Common event 0x002A implemented. <b>0b0</b> Event 0x002A not implemented.	0b0
[9]	ID9	Common event 0x0029 implemented. <b>0b0</b> Event 0x0029 not implemented.	0b0
[8]	ID8	Common event 0x0028 implemented. <b>0b0</b> Event 0x0028 not implemented.	0b0
[7]	ID7	Common event 0x0027 implemented. <b>0b0</b> Event 0x0027 not implemented.	0b0
[6]	ID6	Common event 0x0026 implemented. <b>0b0</b> Event 0x0026 not implemented.	0b0
[5]	ID5	Common event 0x0025 implemented. <b>0b0</b> Event 0x0025 not implemented.	0b0

Bits	Name	Description	Reset
[4]	ID4	Common event 0x0024 implemented. <b>0b0</b> Event 0x0024 not implemented.	0b0
[3]	ID3	Common event 0x0023 implemented. <b>0b0</b> Event 0x0023 not implemented.	0b0
[2]	ID2	Common event 0x0022 implemented. <b>0b0</b> Event 0x0022 not implemented.	0b0
[1]	ID1	Common event 0x0021 implemented. <b>0b0</b> Event 0x0021 not implemented.	0b0
[0]	ID0	Common event 0x0020 implemented. <b>0b0</b> Event 0x0020 not implemented.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xE24	None

This interface is accessible as follows:

#### When IsCorePowered() and AllowExternalPMUAccess()

RO

#### Otherwise

ERROR

#### B.2.2.2.16 CLUSTERPMU\_PMCEID2, Cluster Performance Monitors Common Event Identification register 2

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the range 0x4000 to 0x401F.

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

### Configurations

External register CLUSTERPMU\_PMCEID2 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.15 IMP\\_CLUSTERPMCEID0\\_EL1, Cluster Performance Monitors Common Event Identification register 0](#) on page 783 bits [63:32].

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xE28

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-186: EXT\_CLUSTERPMU\_PMCEID2 bit assignments

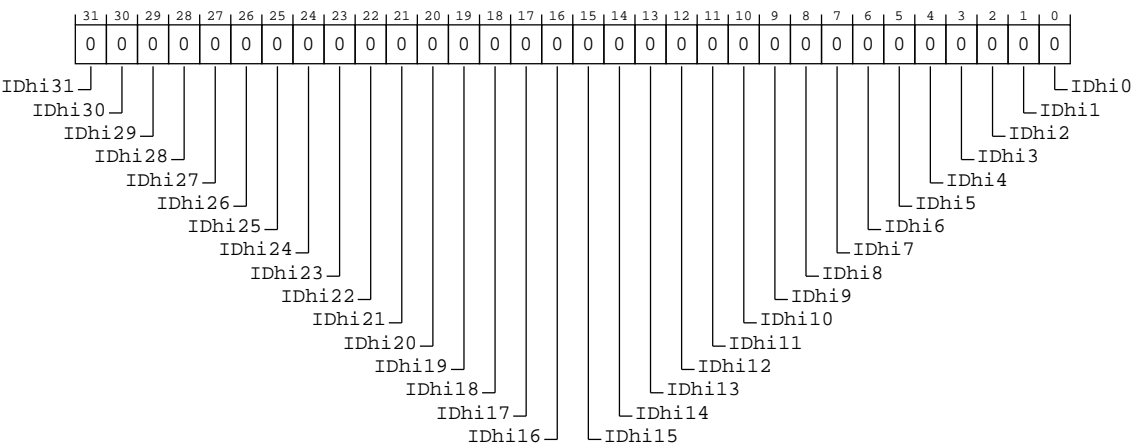


Table B-380: CLUSTERPMU\_PMCEID2 bit descriptions

Bits	Name	Description	Reset
[31]	IDHi31	Common event 0x401F implemented. <b>0b0</b> Event 0x401F not implemented.	0b0
[30]	IDHi30	Common event 0x401E implemented. <b>0b0</b> Event 0x401E not implemented.	0b0
[29]	IDHi29	Common event 0x401D implemented. <b>0b0</b> Event 0x401D not implemented.	0b0

Bits	Name	Description	Reset
[28]	IDHi28	Common event 0x401C implemented. <b>0b0</b> Event 0x401C not implemented.	0b0
[27]	IDHi27	Common event 0x401B implemented. <b>0b0</b> Event 0x401B not implemented.	0b0
[26]	IDHi26	Common event 0x401A implemented. <b>0b0</b> Event 0x401A not implemented.	0b0
[25]	IDHi25	Common event 0x4019 implemented. <b>0b0</b> Event 0x4019 not implemented.	0b0
[24]	IDHi24	Common event 0x4018 implemented. <b>0b0</b> Event 0x4018 not implemented.	0b0
[23]	IDHi23	Common event 0x4017 implemented. <b>0b0</b> Event 0x4017 not implemented.	0b0
[22]	IDHi22	Common event 0x4016 implemented. <b>0b0</b> Event 0x4016 not implemented.	0b0
[21]	IDHi21	Common event 0x4015 implemented. <b>0b0</b> Event 0x4015 not implemented.	0b0
[20]	IDHi20	Common event 0x4014 implemented. <b>0b0</b> Event 0x4014 not implemented.	0b0
[19]	IDHi19	Common event 0x4013 implemented. <b>0b0</b> Event 0x4013 not implemented.	0b0
[18]	IDHi18	Common event 0x4012 implemented. <b>0b0</b> Event 0x4012 not implemented.	0b0
[17]	IDHi17	Common event 0x4011 implemented. <b>0b0</b> Event 0x4011 not implemented.	0b0
[16]	IDHi16	Common event 0x4010 implemented. <b>0b0</b> Event 0x4010 not implemented.	0b0
[15]	IDHi15	Common event 0x400F implemented. <b>0b0</b> Event 0x400F not implemented.	0b0

Bits	Name	Description	Reset
[14]	IDhi14	Common event 0x400E implemented. <b>0b0</b> Event 0x400E not implemented.	0b0
[13]	IDhi13	Common event 0x400D implemented. <b>0b0</b> Event 0x400D not implemented.	0b0
[12]	IDhi12	Common event 0x400C implemented. <b>0b0</b> Event 0x400C not implemented.	0b0
[11]	IDhi11	Common event 0x400B implemented. <b>0b0</b> Event 0x400B not implemented.	0b0
[10]	IDhi10	Common event 0x400A implemented. <b>0b0</b> Event 0x400A not implemented.	0b0
[9]	IDhi9	Common event 0x4009 implemented. <b>0b0</b> Event 0x4009 not implemented.	0b0
[8]	IDhi8	Common event 0x4008 implemented. <b>0b0</b> Event 0x4008 not implemented.	0b0
[7]	IDhi7	Common event 0x4007 implemented. <b>0b0</b> Event 0x4007 not implemented.	0b0
[6]	IDhi6	Common event 0x4006 implemented. <b>0b0</b> Event 0x4006 not implemented.	0b0
[5]	IDhi5	Common event 0x4005 implemented. <b>0b0</b> Event 0x4005 not implemented.	0b0
[4]	IDhi4	Common event 0x4004 implemented. <b>0b0</b> Event 0x4004 not implemented.	0b0
[3]	IDhi3	Common event 0x4003 implemented. <b>0b0</b> Event 0x4003 not implemented.	0b0
[2]	IDhi2	Common event 0x4002 implemented. <b>0b0</b> Event 0x4002 not implemented.	0b0
[1]	IDhi1	Common event 0x4001 implemented. <b>0b0</b> Event 0x4001 not implemented.	0b0



Bits	Name	Description	Reset
[0]	IDhi0	Common event 0x4000 implemented.  <b>0b0</b> Event 0x4000 not implemented.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xE28	None

This interface is accessible as follows:

#### When IsCorePowered() and AllowExternalPMUAccess()

RO

#### Otherwise

ERROR

#### B.2.2.2.17 CLUSTERPMU\_PMCEID3, Cluster Performance Monitors Common Event Identification register 3

Defines which common architectural events and common microarchitectural events are implemented, or counted, using PMU events in the range 0x4020 to 0x403F.

When the value of a bit in the register is 1 the corresponding common event is implemented and counted.

### Configurations

External register CLUSTERPMU\_PMCEID3 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.16 IMP\\_CLUSTERPMCEID1\\_EL1, Cluster Performance Monitors Common Event Identification register 1](#) on page 790 bits [63:32].

### Attributes

#### Width

32

#### Component

CLUSTERPMU

#### Register offset

0xE2C

#### Access type

See bit descriptions

#### Reset value

0000 0000 0000 0000 0000 0000 0000 0000

## Bit descriptions

Figure B-187: EXT\_CLUSTERPMU\_PMCEID3 bit assignments

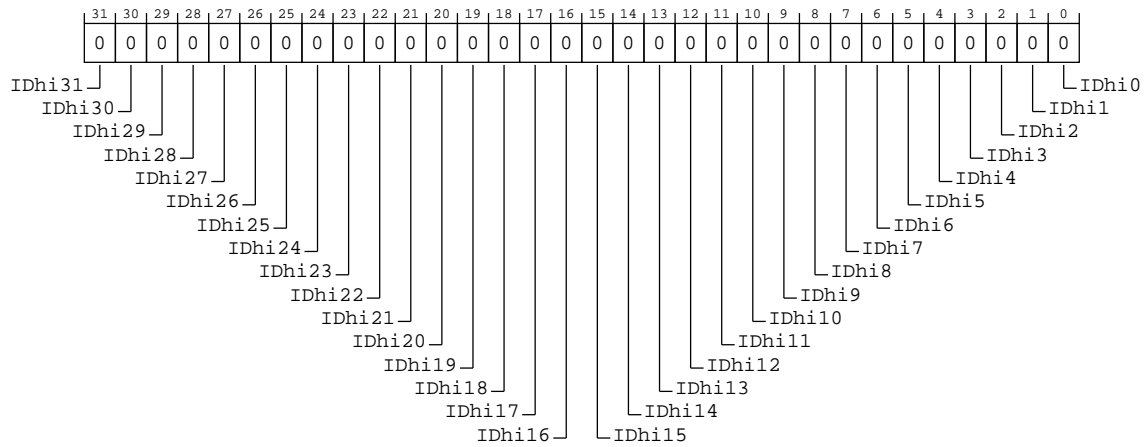


Table B-382: CLUSTERPMU\_PMCEID3 bit descriptions

Bits	Name	Description	Reset
[31]	IDhi31	Common event 0x403F implemented. <b>0b0</b> Event 0x403F not implemented.	0b0
[30]	IDhi30	Common event 0x403E implemented. <b>0b0</b> Event 0x403E not implemented.	0b0
[29]	IDhi29	Common event 0x403D implemented. <b>0b0</b> Event 0x403D not implemented.	0b0
[28]	IDhi28	Common event 0x403C implemented. <b>0b0</b> Event 0x403C not implemented.	0b0
[27]	IDhi27	Common event 0x403B implemented. <b>0b0</b> Event 0x403B not implemented.	0b0
[26]	IDhi26	Common event 0x403A implemented. <b>0b0</b> Event 0x403A not implemented.	0b0
[25]	IDhi25	Common event 0x4039 implemented. <b>0b0</b> Event 0x4039 not implemented.	0b0
[24]	IDhi24	Common event 0x4038 implemented. <b>0b0</b> Event 0x4038 not implemented.	0b0

Bits	Name	Description	Reset
[23]	IDhi23	Common event 0x4037 implemented. <b>0b0</b> Event 0x4037 not implemented.	0b0
[22]	IDhi22	Common event 0x4036 implemented. <b>0b0</b> Event 0x4036 not implemented.	0b0
[21]	IDhi21	Common event 0x4035 implemented. <b>0b0</b> Event 0x4035 not implemented.	0b0
[20]	IDhi20	Common event 0x4034 implemented. <b>0b0</b> Event 0x4034 not implemented.	0b0
[19]	IDhi19	Common event 0x4033 implemented. <b>0b0</b> Event 0x4033 not implemented.	0b0
[18]	IDhi18	Common event 0x4032 implemented. <b>0b0</b> Event 0x4032 not implemented.	0b0
[17]	IDhi17	Common event 0x4031 implemented. <b>0b0</b> Event 0x4031 not implemented.	0b0
[16]	IDhi16	Common event 0x4030 implemented. <b>0b0</b> Event 0x4030 not implemented.	0b0
[15]	IDhi15	Common event 0x402F implemented. <b>0b0</b> Event 0x402F not implemented.	0b0
[14]	IDhi14	Common event 0x402E implemented. <b>0b0</b> Event 0x402E not implemented.	0b0
[13]	IDhi13	Common event 0x402D implemented. <b>0b0</b> Event 0x402D not implemented.	0b0
[12]	IDhi12	Common event 0x402C implemented. <b>0b0</b> Event 0x402C not implemented.	0b0
[11]	IDhi11	Common event 0x402B implemented. <b>0b0</b> Event 0x402B not implemented.	0b0
[10]	IDhi10	Common event 0x402A implemented. <b>0b0</b> Event 0x402A not implemented.	0b0

Bits	Name	Description	Reset
[9]	IDhi9	Common event 0x4029 implemented. <b>0b0</b> Event 0x4029 not implemented.	0b0
[8]	IDhi8	Common event 0x4028 implemented. <b>0b0</b> Event 0x4028 not implemented.	0b0
[7]	IDhi7	Common event 0x4027 implemented. <b>0b0</b> Event 0x4027 not implemented.	0b0
[6]	IDhi6	Common event 0x4026 implemented. <b>0b0</b> Event 0x4026 not implemented.	0b0
[5]	IDhi5	Common event 0x4025 implemented. <b>0b0</b> Event 0x4025 not implemented.	0b0
[4]	IDhi4	Common event 0x4024 implemented. <b>0b0</b> Event 0x4024 not implemented.	0b0
[3]	IDhi3	Common event 0x4023 implemented. <b>0b0</b> Event 0x4023 not implemented.	0b0
[2]	IDhi2	Common event 0x4022 implemented. <b>0b0</b> Event 0x4022 not implemented.	0b0
[1]	IDhi1	Common event 0x4021 implemented. <b>0b0</b> Event 0x4021 not implemented.	0b0
[0]	IDhi0	Common event 0x4020 implemented. <b>0b0</b> Event 0x4020 not implemented.	0b0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xE2C	None

This interface is accessible as follows:

**When IsCorePowered() and AllowExternalPMUAccess()**

RO

**Otherwise**

ERROR

B.2.2.2.18 CLUSTERPMU\_PMMIR, Cluster Performance Monitors Machine Identification Register

No STALL\_SLOT events for the Cluster PMU.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

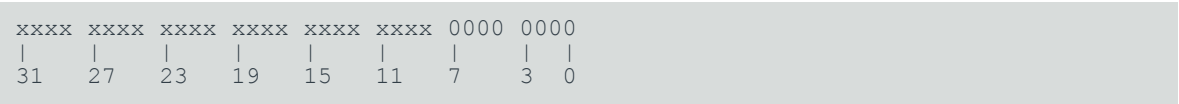
Register offset

0xE40

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-188: EXT\_CLUSTERPMU\_PMMIR bit assignments

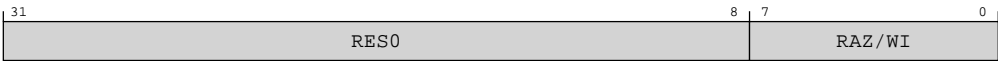


Table B-384: CLUSTERPMU\_PMMIR bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERPMU	0xE40	None

This interface is accessible as follows:

**When !IsCorePowered() or !AllowExternalPMUAccess()**  
ERROR

**Otherwise**  
RO

B.2.2.2.19 CLUSTERPMU\_PMITCTRL, Cluster Performance Monitors Integration mode Control register

No functional/integration mode switching implemented for the Cluster PMU.

**Configurations**

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMITCTRL. Otherwise, direct accesses to CLUSTERPMU\_PMITCTRL are UNDEFINED.

**Attributes**

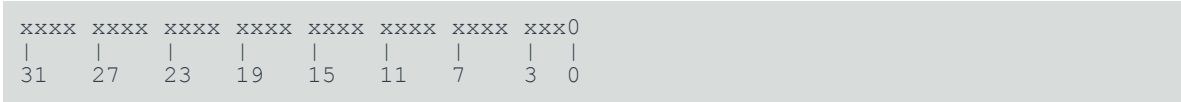
**Width**  
32

**Component**  
CLUSTERPMU

**Register offset**  
0xF00

**Access type**  
See bit descriptions

**Reset value**



Where the reset reads xxxx, see individual bits.

**Bit descriptions**

**Figure B-189: EXT\_CLUSTERPMU\_PMITCTRL bit assignments**

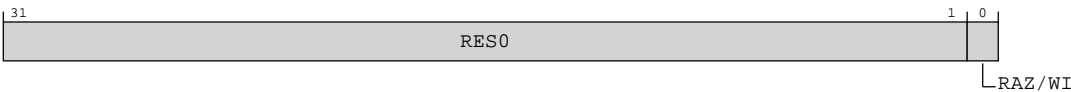


Table B-386: CLUSTERPMU\_PMITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERPMU	0xF00	None

This interface is accessible as follows:

When IsCorePowered()

RW

Otherwise

ImplementationDefined

B.2.2.2.20 CLUSTERPMU\_PMCLAIMSET\_EL1, Cluster Performance Monitors Claim Set register

Used by software to set CLAIM bits to 1.

Configurations

External register CLUSTERPMU\_PMCLAIMSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.17 IMP\\_CLUSTERPMCLAIMSET\\_EL1, Cluster Performance Monitors Claim Set register](#) on page 797 bits [31:0].

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFA0

Access type

RW1S

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-190: EXT\_CLUSTERPMU\_PMCLAIMSET\_EL1 bit assignments

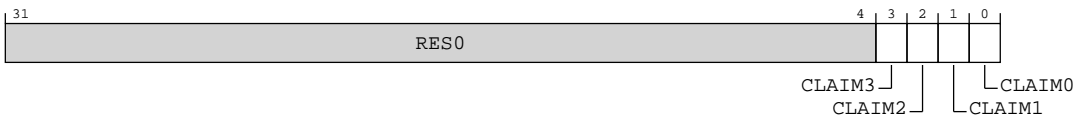


Table B-388: CLUSTERPMU\_PMCLAIMSET\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	CLAIM tag set bit.  <b>0b0</b> No action.  <b>0b1</b> Indirectly set claim bit to 1.	xxxx

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFA0	None

This interface is accessible as follows:

When IsCorePowered()

RW

Otherwise

ERROR

B.2.2.2.21 CLUSTERPMU\_PMCLAIMCLR\_EL1, Cluster Performance Monitors Claim Clear register

Used by software to read the values of the CLAIM bits, and to clear these bits to 0.

Configurations

External register CLUSTERPMU\_PMCLAIMCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.18 IMP\\_CLUSTERPMCLAIMCLR\\_EL1, Cluster Performance Monitors Claim Clear register](#) on page 799 bits [31:0].



Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFA4

Access type

RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-191: EXT\_CLUSTERPMU\_PMCLAIMCLR\_EL1 bit assignments

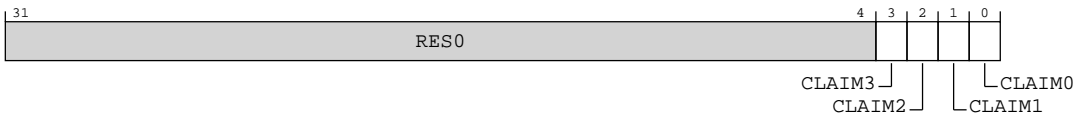


Table B-390: CLUSTERPMU\_PMCLAIMCLR\_EL1 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	CLAIM tag clear bit.  <b>0b0</b> No action.  <b>0b1</b> Indirectly clear claim bit to 0.	xxxx

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFA4	None

This interface is accessible as follows:

When IsCorePowered()

RW

Otherwise

ERROR

B.2.2.2.22 CLUSTERPMU\_PMDEVAFF0, Cluster Performance Monitors Device Affinity register 0

Allows a debugger to determine which PE in a multiprocessor system the Performance Monitor component relates to.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFA8

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0

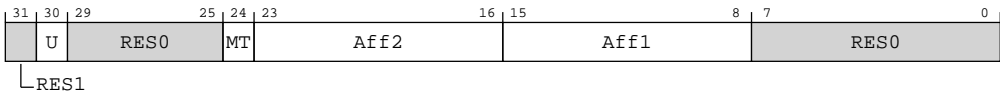


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-192: EXT\_CLUSTERPMU\_PMDEVAFF0 bit assignments



**Table B-392: CLUSTERPMU\_PMDEVAFF0 bit descriptions**

Bits	Name	Description	Reset
[31]	RES1	Reserved	RES1
[30]	U	Uniprocessor/Multiprocessor system.  <b>0b0</b> Processor is part of a multiprocessor system.	x
[29:25]	RES0	Reserved	RES0
[24]	MT	Indicates whether the lowest level of affinity consists of logical PEs that are implemented using a multithreading type approach.  <b>0b1</b> Performance of PEs at the lowest affinity level is very interdependent.	x
[23:16]	Aff2	Affinity level 2. Value read from the CFGMPIDRAFF2 configuration pins.	8 {x}
[15:8]	Aff1	Affinity level 1.  <b>0b10000000</b> Cluster PMU.	8 {x}
[7:0]	RES0	Reserved	RES0

### Accessibility

Component	Offset	Range
CLUSTERPMU	0xFA8	None

This interface is accessible as follows:

#### When IsCorePowered()

RO

#### Otherwise

ERROR

#### B.2.2.2.23 CLUSTERPMU\_PMDEVAFF1, Cluster Performance Monitors Device Affinity register 1

Allows a debugger to determine which PE in a multiprocessor system the Performance Monitor component relates to.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

CLUSTERPMU

Register offset

0xFAC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-193: EXT\_CLUSTERPMU\_PMDEVAFF1 bit assignments



Table B-394: CLUSTERPMU\_PMDEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	Aff3	Affinity level 3. Value read from the CFGMPIDRAFF3 configuration pins.	8 {x}

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFAC	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.24 CLUSTERPMU\_PMLAR, Cluster Performance Monitors Lock Access Register

No software locking implemented for the Cluster PMU.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFB0

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-194: EXT\_CLUSTERPMU\_PMLAR bit assignments

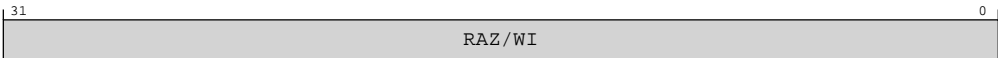


Table B-396: CLUSTERPMU\_PMLAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFB0	None

This interface is accessible as follows:

When IsCorePowered()

WO

Otherwise

ERROR

B.2.2.2.25 CLUSTERPMU\_PMLSR, Cluster Performance Monitors Lock Status Register

No software locking implemented for the Cluster PMU.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFB4

Access type

See bit descriptions

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-195: EXT\_CLUSTERPMU\_PMLSR bit assignments

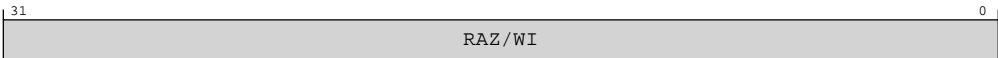


Table B-398: CLUSTERPMU\_PMLSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFB4	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.26 CLUSTERPMU\_PMAUTHSTATUS, Cluster Performance Monitors Authentication Status register

Provides information about the state of the authentication interface for Performance Monitors.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

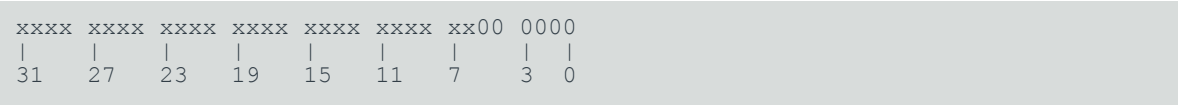
Register offset

0xFB8

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-196: EXT\_CLUSTERPMU\_PMAUTHSTATUS bit assignments

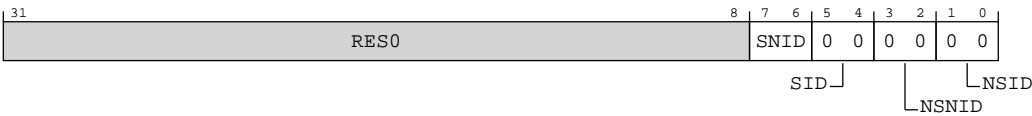


Table B-400: CLUSTERPMU\_PMAUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure Non-invasive Debug.  0b10 Implemented and disabled. ExternalSecureNoninvasiveDebugEnabled() == FALSE.  0b11 Implemented and enabled. ExternalSecureNoninvasiveDebugEnabled() == TRUE.	xx
[5:4]	SID	Secure Invasive Debug.  0b00 Debug level is not supported	0b00
[3:2]	NSNID	Non-secure Non-invasive Debug.  0b00 Debug level is not supported.	0b00

Bits	Name	Description	Reset
[1:0]	NSID	Non-secure Invasive Debug.  0b00  Debug level is not supported.	0b00

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFB8	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.27 CLUSTERPMU\_PMDEVARCH, Cluster Performance Monitors Device Architecture register

Identifies the programmers' model architecture of the Performance Monitor component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFBC

Access type

See bit descriptions

Reset value

0100 0111 0111 0000 0010 1010 0001 0110



Bit descriptions

Figure B-197: EXT\_CLUSTERPMU\_PMDEVARCH bit assignments

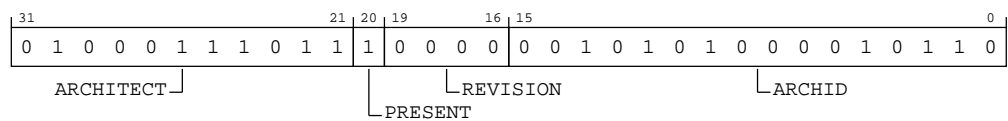


Table B-402: CLUSTERPMU\_PMDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect.  0b01000111011 JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	Present.  0b1 DEVARCH information present.	0b1
[19:16]	REVISION	Revision.  0b0000 Revision 0.	0b0000
[15:0]	ARCHID	Architecture ID.  0b0010101000010110 Processor Performance Monitor (PMU) architecture PMUv3.	0x2A16

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFBC	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.28 CLUSTERPMU\_PMDEVID, Cluster Performance Monitors Device ID register

Provides information about features of the Performance Monitors implementation.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFC8

Access type

See bit descriptions

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-198: EXT\_CLUSTERPMU\_PMDEVID bit assignments



Table B-404: CLUSTERPMU\_PMDEVID bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	PCSample	Indicates the level of PC Sample-based Profiling support using Performance Monitors registers. <b>0b0000</b> PC Sample-based Profiling Extension is not implemented for the Cluster PMU.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFC8	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise  
ERROR

B.2.2.2.29 CLUSTERPMU\_PMDEVTYPE, Cluster Performance Monitors Device Type register

Indicates to a debugger that this component is part of a processor performance monitor interface.

Configurations

This register is present only when `ImpDefBool("IMPLEMENTED_CLUSTERPMU_PMDEVTYPE`. Otherwise, direct accesses to `CLUSTERPMU_PMDEVTYPE` are `UNDEFINED`.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFCC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-199: EXT\_CLUSTERPMU\_PMDEVTYPE bit assignments

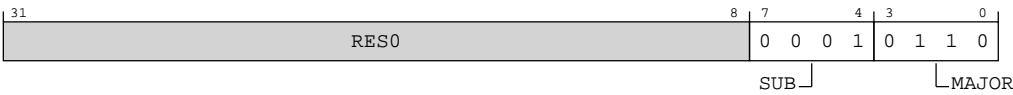


Table B-406: CLUSTERPMU\_PMDEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	SUB	Subtype. <b>0b0001</b> Associated with a processor.	0b0001
[3:0]	MAJOR	Major type. <b>0b0110</b> Performance Monitor.	0b0110

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFCC	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.2.30 CLUSTERPMU\_PMPIDR4, Cluster Performance Monitors Peripheral Identification Register 4

Provides information to identify a Performance Monitor component.

For more information see.

Configurations

This register is required for CoreSight compliance.

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMPIDR4. Otherwise, direct accesses to CLUSTERPMU\_PMPIDR4 are UNDEFINED.

Attributes

**Width**

32

**Component**

CLUSTERPMU

**Register offset**

0xFD0

**Access type**

See bit descriptions

**Reset value**

```
xxxx xxxx xxxx xxxx xxxx xxxx 0000 0100
```



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-200: EXT\_CLUSTERPMU\_PMPIDR4 bit assignments

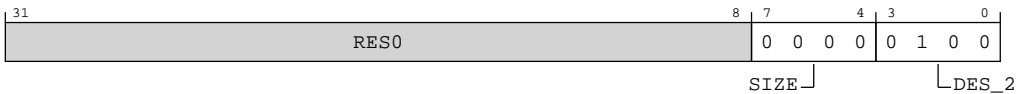


Table B-408: CLUSTERPMU\_PMPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count.  0b0000 The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code.  0b0100 Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFD0	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.31 CLUSTERPMU\_PMPIDR0, Cluster Performance Monitors Peripheral Identification Register 0

Provides information to identify a Performance Monitor component.

For more information see.

Configurations

This register is required for CoreSight compliance.

This register is present only when `ImpDefBool("IMPLEMENTED_CLUSTERPMU_PMPIDR0`. Otherwise, direct accesses to `CLUSTERPMU_PMPIDR0` are UNDEFINED.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFE0

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-201: EXT\_CLUSTERPMU\_PMPIDR0 bit assignments



Table B-410: CLUSTERPMU\_PMPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b00010100 Cortex-R82AE Cluster PMU. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFE0	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.32 CLUSTERPMU\_PMPIDR1, Cluster Performance Monitors Peripheral Identification Register 1

Provides information to identify a Performance Monitor component.

For more information see.

Configurations

This register is required for CoreSight compliance.

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMPIDR1. Otherwise, direct accesses to CLUSTERPMU\_PMPIDR1 are UNDEFINED.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFE4

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	1101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-202: EXT\_CLUSTERPMU\_PMPIDR1 bit assignments



Table B-412: CLUSTERPMU\_PMPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0]. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b1101</b> Cortex-R82AE Cluster PMU. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFE4	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.33 CLUSTERPMU\_PMPIDR2, Cluster Performance Monitors Peripheral Identification Register 2

Provides information to identify a Performance Monitor component.

For more information see.

Configurations

This register is required for CoreSight compliance.

This register is present only when `ImpDefBool("IMPLEMENTED_CLUSTERPMU_PMPIDR2`. Otherwise, direct accesses to CLUSTERPMU\_PMPIDR2 are UNDEFINED.

Attributes

Width

32



**Component**  
CLUSTERPMU

**Register offset**  
0xFE8

**Access type**  
See bit descriptions

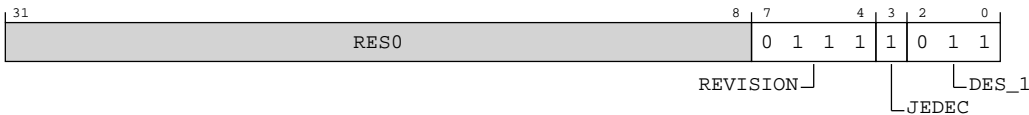
**Reset value**



Where the reset reads xxxx, see individual bits.

**Bit descriptions**

**Figure B-203: EXT\_CLUSTERPMU\_PMPIDR2 bit assignments**



**Table B-414: CLUSTERPMU\_PMPIDR2 bit descriptions**

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision. <b>0b0111</b> Revision 7.	0b0111
[3]	JEDEC	<b>RAO</b> . Indicates a JEP106 identity code is used. <b>0b1</b> JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011. <b>0b011</b> Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

**Accessibility**

Component	Offset	Range
CLUSTERPMU	0xFE8	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

**B.2.2.2.34 CLUSTERPMU\_PMPIDR3, Cluster Performance Monitors Peripheral Identification Register 3**

Provides information to identify a Performance Monitor component.

For more information see.

**Configurations**

This register is required for CoreSight compliance.

This register is present only when `ImpDefBool("IMPLEMENTED_CLUSTERPMU_PMPIDR3`. Otherwise, direct accesses to CLUSTERPMU\_PMPIDR3 are UNDEFINED.

**Attributes**

**Width**

32

**Component**

CLUSTERPMU

**Register offset**

0xFEC

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-204: EXT\_CLUSTERPMU\_PMPIDR3 bit assignments



Table B-416: CLUSTERPMU\_PMPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes. <b>0b0000</b> No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified. <b>0b0000</b> The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFEC	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.35 CLUSTERPMU\_PMCIDR0, Cluster Performance Monitors Component Identification Register 0

Provides information to identify a Performance Monitor component.

For more information see .

Configurations

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMCIDR0. Otherwise, direct accesses to CLUSTERPMU\_PMCIDR0 are UNDEFINED.

Attributes

Width

32


**Component**  
CLUSTERPMU

**Register offset**  
0xFF0

**Access type**  
See bit descriptions

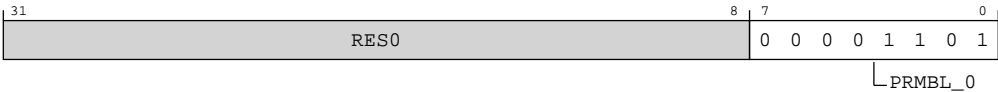
**Reset value**



 Where the reset reads xxxx, see individual bits.

**Bit descriptions**

**Figure B-205: EXT\_CLUSTERPMU\_PMCIDR0 bit assignments**



**Table B-418: CLUSTERPMU\_PMCIDR0 bit descriptions**

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble.  0b00001101 CoreSight component identification preamble.	0x0D

**Accessibility**

Component	Offset	Range
CLUSTERPMU	0xFF0	None

This interface is accessible as follows:

**When IsCorePowered()**  
RO

**Otherwise**  
ERROR

B.2.2.2.36 CLUSTERPMU\_PMCIDR1, Cluster Performance Monitors Component Identification Register 1

Provides information to identify a Performance Monitor component.

For more information see .

Configurations

This register is present only when `ImpDefBool("IMPLEMENTED_CLUSTERPMU_PMCIDR1`. Otherwise, direct accesses to CLUSTERPMU\_PMCIDR1 are UNDEFINED.

Attributes

Width

32

Component

CLUSTERPMU

Register offset

0xFF4

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-206: EXT\_CLUSTERPMU\_PMCIDR1 bit assignments

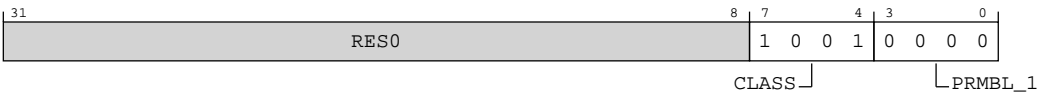


Table B-420: CLUSTERPMU\_PMCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	Component class. <b>0b1001</b> CoreSight debug component.	0b1001

Bits	Name	Description	Reset
[3:0]	PRMBL_1	Preamble.  <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFF4	None

This interface is accessible as follows:

**When IsCorePowered()**

RO

**Otherwise**

ERROR

B.2.2.2.37 CLUSTERPMU\_PMCIDR2, Cluster Performance Monitors Component Identification Register 2

Provides information to identify a Performance Monitor component.

For more information see .

Configurations

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMCIDR2. Otherwise, direct accesses to CLUSTERPMU\_PMCIDR2 are UNDEFINED.

Attributes

**Width**

32

**Component**

CLUSTERPMU

**Register offset**

0xFF8

**Access type**

See bit descriptions

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0101
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-207: EXT\_CLUSTERPMU\_PMCIDR2 bit assignments

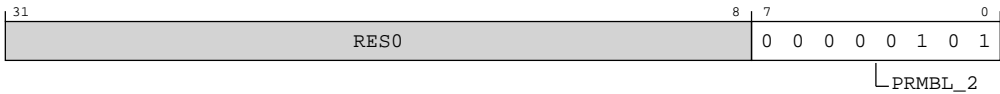


Table B-422: CLUSTERPMU\_PMCIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble.  0b00000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFF8	None

This interface is accessible as follows:

When IsCorePowered()

RO

Otherwise

ERROR

B.2.2.2.38 CLUSTERPMU\_PMCIDR3, Cluster Performance Monitors Component Identification Register 3

Provides information to identify a Performance Monitor component.

For more information see .

Configurations

This register is present only when ImpDefBool("IMPLEMENTED\_CLUSTERPMU\_PMCIDR3. Otherwise, direct accesses to CLUSTERPMU\_PMCIDR3 are UNDEFINED.

Attributes

Width

32

Component

CLUSTERPMU

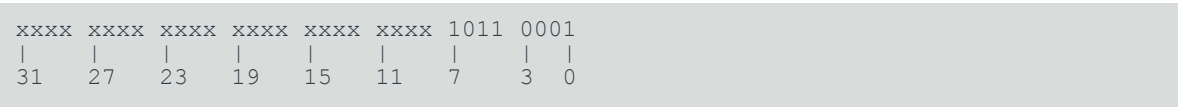
Register offset

0xFFC

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-208: EXT\_CLUSTERPMU\_PMCIDR3 bit assignments



Table B-424: CLUSTERPMU\_PMCIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble. <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
CLUSTERPMU	0xFFC	None

This interface is accessible as follows:

When IsCorePowered()

RO



Otherwise  
ERROR

B.2.2.3 External DBROM register description

This section includes the register descriptions for all memory-mapped DBROM registers that are accessed for the DebugBlok.

B.2.2.3.1 DBROM\_ROMENTRY0, DebugBlock ROM table Entry 0

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x000

Access type

RO

Reset value

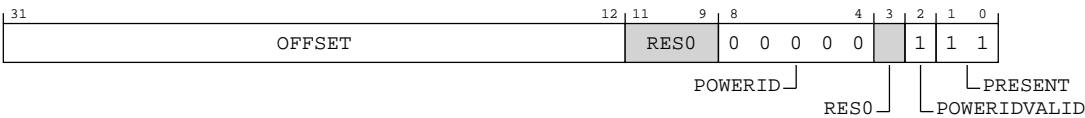
xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	0000	x111
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-209: EXT\_DBROM\_ROMENTRY0 bit assignments



**Table B-426: DBROM\_ROMENTRY0 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000001</b> Cluster ROM table at address 0x0_1000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000100000000</b> Cluster ROM table at address 0x20_0000.</p>	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	<p>The power domain ID of the component.</p> <p><b>0b00000</b> PDCLUSTER power domain.</p>	0b00000
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b1</b> The POWERID field provides a power domain ID.</p>	0b1
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

### Accessibility

Component	Offset	Range
DBROM	0x000	None

This interface is accessible as follows:

RO

#### B.2.2.3.2 DBROM\_ROMENTRY1, DebugBlock ROM table Entry 1

Provides the address offset for one CoreSight component.

### Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x004

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-210: EXT\_DBROM\_ROMENTRY1 bit assignments

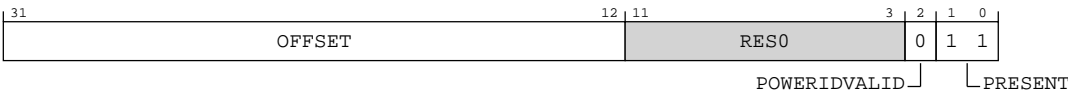


Table B-428: DBROM\_ROMENTRY1 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:</p> <p>Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000000000100</b></p> <p>Cluster CTI at address 0x0_4000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:</p> <p>Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000001000110000</b></p> <p>Cluster CTI at address 0x23_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID.  <b>0b0</b> A power domain ID is not provided.	0b0
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table.  <b>0b11</b> The ROM Entry is present.	0b11

Accessibility

Component	Offset	Range
DBROM	0x004	None

This interface is accessible as follows:

RO

B.2.2.3.3 DBROM\_ROMENTRY2, DebugBlock ROM table Entry 2

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x008

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x011
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-211: EXT\_DBROM\_ROMENTRY2 bit assignments

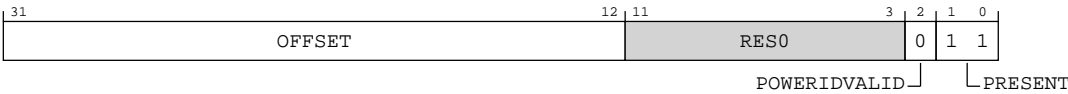


Table B-430: DBROM\_ROMENTRY2 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000001010</b> Core 0 CTI at address 0x0_A000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000001000000000</b> Core 0 CTI at address 0x10_0000.</p>	20{x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

Accessibility

Component	Offset	Range
DBROM	0x008	None

This interface is accessible as follows:

RO

B.2.2.3.4 DBROM\_ROMENTRY3, DebugBlock ROM table Entry 3

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x00C

Access type

RO

Reset value

When NUM\_CORES >= 2

xxxx xxxx xxxx xxxx xxxx xxxx x0xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

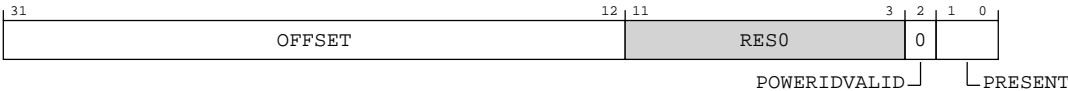


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 2

Figure B-212: EXT\_DBROM\_ROMENTRY3 bit assignments



### Table B-432: DBROM\_ROMENTRY3 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:  Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000000010000</b></p> <p>Core 1 CTI at address 0x1_0000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:  Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000100010000</b></p> <p>Core 1 CTI at address 0x11_0000.</p>	20{x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p><b>When CFGCEMODE == 3</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>10</b></p> <p>The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.</p> <p><b>Otherwise</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>11</b></p> <p>The ROM Entry is present.</p>	xx

### Figure B-213: EXT\_DBROM\_ROMENTRY3 bit assignments



### Table B-433: DBROM\_ROMENTRY3 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

## Accessibility

Component	Offset	Range
DBROM	0x00C	None

This interface is accessible as follows:

RO

B.2.2.3.5 DBROM\_ROMENTRY4, DebugBlock ROM table Entry 4

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x010

Access type

RO

Reset value

When NUM\_CORES >= 3

xxxx xxxx xxxx xxxx xxxx xxxx xxxx x011  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

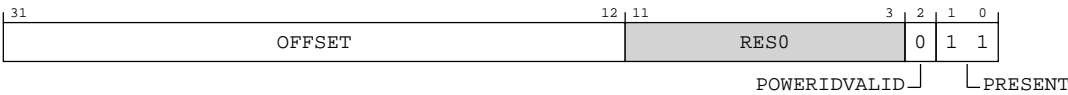


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 3

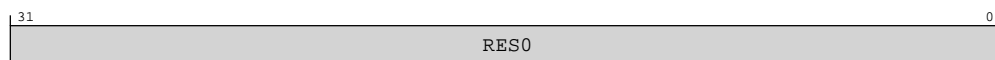
Figure B-214: EXT\_DBROM\_ROMENTRY4 bit assignments





**Table B-435: DBROM\_ROMENTRY4 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000000010110</b> Core 2 CTI at address 0x1_6000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000100100000</b> Core 2 CTI at address 0x12_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

**Figure B-215: EXT\_DBROM\_ROMENTRY4 bit assignments****Table B-436: DBROM\_ROMENTRY4 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

**Accessibility**

Component	Offset	Range
DBROM	0x010	None

This interface is accessible as follows:

RO

B.2.2.3.6 DBROM\_ROMENTRY5, DebugBlock ROM table Entry 5

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x014

Access type

RO

Reset value

When NUM\_CORES >= 4

xxxx xxxx xxxx xxxx xxxx xxxx x0xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

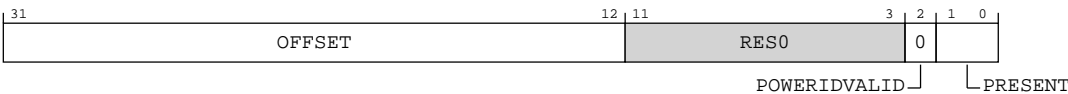


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 4

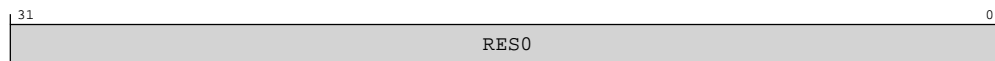
Figure B-216: EXT\_DBROM\_ROMENTRY5 bit assignments



### Table B-438: DBROM\_ROMENTRY5 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:  Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000000011100</b></p> <p>Core 3 CTI at address 0x1_C000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:  Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000100110000</b></p> <p>Core 3 CTI at address 0x13_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p><b>When CFGCEMODE == 3</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>10</b></p> <p>The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.</p> <p><b>Otherwise</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>11</b></p> <p>The ROM Entry is present.</p>	xx

**Figure B-217: EXT\_DBROM\_ROMENTRY5 bit assignments**



### Table B-439: DBROM\_ROMENTRY5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

## Accessibility

Component	Offset	Range
DBROM	0x014	None

This interface is accessible as follows:

RO

B.2.2.3.7 DBROM\_ROMENTRY6, DebugBlock ROM table Entry 6

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x018

Access type

RO

Reset value

When NUM\_CORES >= 5

xxxx xxxx xxxx xxxx xxxx xxxx xxxx x011  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

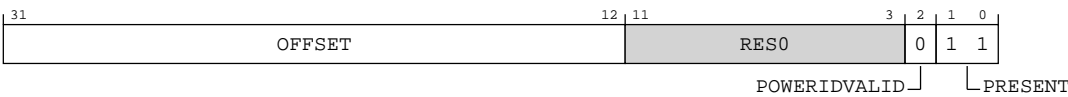


Where the reset reads xxxx, see individual bits.

Bit descriptions

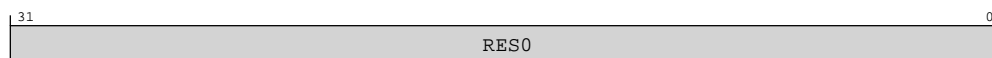
When NUM\_CORES >= 5

Figure B-218: EXT\_DBROM\_ROMENTRY6 bit assignments



**Table B-441: DBROM\_ROMENTRY6 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000000000100010</b> Core 4 CTI at address 0x2_2000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000101000000</b> Core 4 CTI at address 0x14_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

**Figure B-219: EXT\_DBROM\_ROMENTRY6 bit assignments****Table B-442: DBROM\_ROMENTRY6 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

### Accessibility

Component	Offset	Range
DBROM	0x018	None

This interface is accessible as follows:

RO

B.2.2.3.8 DBROM\_ROMENTRY7, DebugBlock ROM table Entry 7

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x01C

Access type

RO

Reset value

When NUM\_CORES >= 6

xxxx xxxx xxxx xxxx xxxx xxxx x0xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx

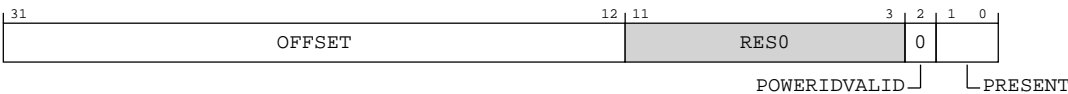


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 6

Figure B-220: EXT\_DBROM\_ROMENTRY7 bit assignments



### Table B-444: DBROM\_ROMENTRY7 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:            Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000000101000</b></p> <p>Core 5 CTI at address 0x2_8000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation:            Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000101010000</b></p> <p>Core 5 CTI at address 0x15_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p><b>When CFGCEMODE == 3</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>10</b></p> <p>The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.</p> <p><b>Otherwise</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>11</b></p> <p>The ROM Entry is present.</p>	xx

**Figure B-221: EXT\_DBROM\_ROMENTRY7 bit assignments**



### Table B-445: DBROM\_ROMENTRY7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

## Accessibility

Component	Offset	Range
DBROM	0x01C	None

This interface is accessible as follows:

RO

B.2.2.3.9 DBROM\_ROMENTRY8, DebugBlock ROM table Entry 8

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x020

Access type

RO

Reset value

When NUM\_CORES >= 7

xxxx xxxx xxxx xxxx xxxx xxxx xxxx x011  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

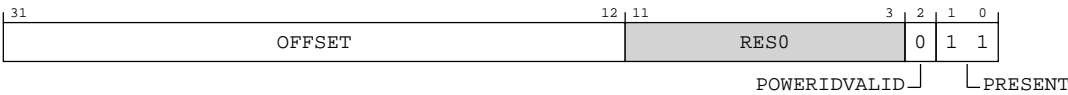


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 7

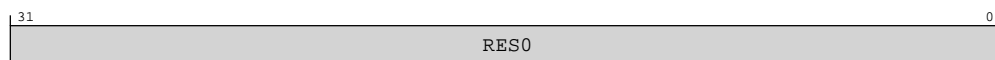
Figure B-222: EXT\_DBROM\_ROMENTRY8 bit assignments





**Table B-447: DBROM\_ROMENTRY8 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000101110</b> Core 6 CTI at address 0x2_E000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000101100000</b> Core 6 CTI at address 0x16_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

**Figure B-223: EXT\_DBROM\_ROMENTRY8 bit assignments****Table B-448: DBROM\_ROMENTRY8 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

### Accessibility

Component	Offset	Range
DBROM	0x020	None

This interface is accessible as follows:

RO

B.2.2.3.10 DBROM\_ROMENTRY9, DebugBlock ROM table Entry 9

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0x024

Access type

RO

Reset value

When NUM\_CORES == 8

xxxx xxxx xxxx xxxx xxxx xxxx xxxx x0xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

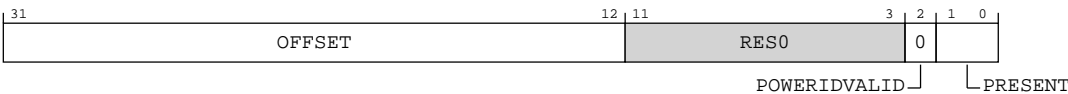


Where the reset reads xxxx, see individual bits.

Bit descriptions

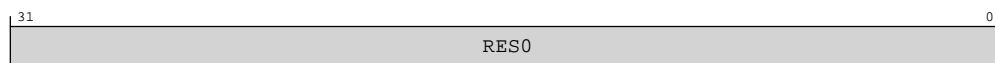
When NUM\_CORES == 8

Figure B-224: EXT\_DBROM\_ROMENTRY9 bit assignments



**Table B-450: DBROM\_ROMENTRY9 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000110100</b> Core 7 CTI at address 0x3_4000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000101110000</b> Core 7 CTI at address 0x17_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p><b>When CFGCEMODE == 3</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>10</b></p> <p>The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.</p> <p><b>Otherwise</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>11</b></p> <p>The ROM Entry is present.</p>	xx

**Figure B-225: EXT\_DBROM\_ROMENTRY9 bit assignments****Table B-451: DBROM\_ROMENTRY9 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

**Accessibility**

Component	Offset	Range
DBROM	0x024	None

This interface is accessible as follows:

RO

B.2.2.3.11 DBROM\_DBGPCR0, DebugBlock ROM table Debug Power Control Register 0

Controls power requests for PDCLUSTER.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xA00

Access type

RW

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-226: EXT\_DBROM\_DBGPCR0 bit assignments

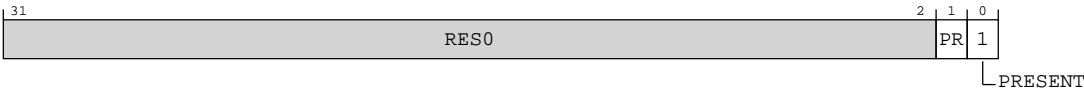


Table B-453: DBROM\_DBGPCR0 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1]	PR	Power Request.  <b>0b0</b> Power is not requested for PDCLUSTER.  <b>0b1</b> Power is requested for PDCLUSTER.	x
[0]	PRESENT	Power request implemented.  <b>0b1</b> Power request for PDCLUSTER is implemented.	0b1

Accessibility

Component	Offset	Range
DBROM	0xA00	None

This interface is accessible as follows:

RW

B.2.2.3.12 DBROM\_DBGPSR0, DebugBlock ROM table Debug Power Status Register 0

Indicates the power status for PDCLUSTER.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xA80

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-227: EXT\_DBROM\_DBGPSR0 bit assignments

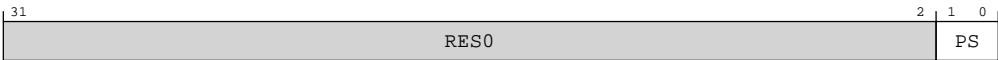


Table B-455: DBROM\_DBGPSR0 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1:0]	PS	Power Status.  0b00 PDCLUSTER might not be powered.  0b01 PDCLUSTER is powered.	xx

Accessibility

Component	Offset	Range
DBROM	0xA80	None

This interface is accessible as follows:

RO

B.2.2.3.13 DBROM\_PRIDR0, DebugBlock ROM table Power Request ID Register 0

Indicates the features of the power request functionality.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xC00

Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-228: EXT\_DBROM\_PRIDR0 bit assignments

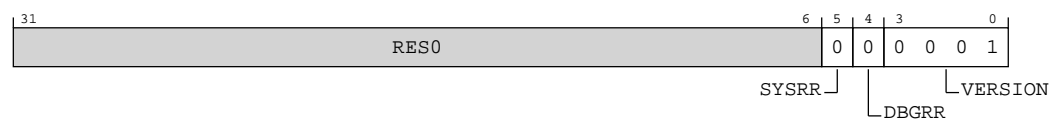


Table B-457: DBROM\_PRIDR0 bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	SYSRR	System reset request functionality present.  0b0 The system reset request functionality is not implemented.	0b0
[4]	DBGRR	Debug reset request functionality present.  0b0 The debug reset request functionality is not implemented.	0b0
[3:0]	VERSION	Version of the power request functionality.  0b0001 The power request functionality version 0, and the ext-DBROM_DBGPCR0, ext-DBROM_DBGPSR0, which provide controls for power requests, are implemented.	0b0001

Accessibility

Component	Offset	Range
DBROM	0xC00	None

This interface is accessible as follows:

RO

B.2.2.3.14 DBROM\_ITCTRL, DebugBlock ROM table Integration Mode Control Register

No functional/integration mode switching implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

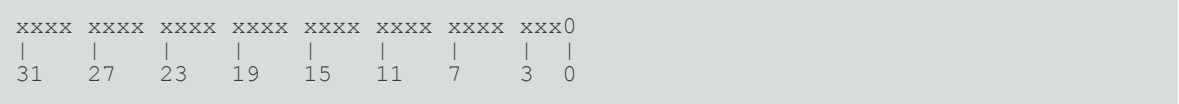
Register offset

0xF00

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-229: EXT\_DBROM\_ITCTRL bit assignments

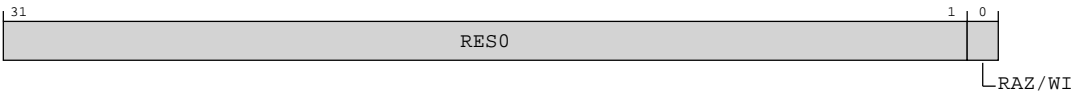


Table B-459: DBROM\_ITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
DBROM	0xF00	None



This interface is accessible as follows:

RW

B.2.2.3.15 DBROM\_CLAIMSET, DebugBlock ROM table Claim Tag Set Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFA0

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-230: EXT\_DBROM\_CLAIMSET bit assignments

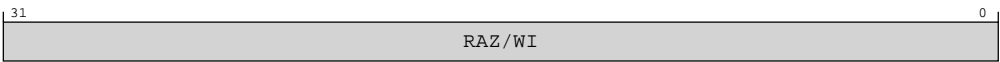


Table B-461: DBROM\_CLAIMSET bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
DBROM	0xFA0	None

This interface is accessible as follows:

RW

B.2.2.3.16 DBROM\_CLAIMCLR, DebugBlock ROM table Claim Tag Clear Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFA4

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-231: EXT\_DBROM\_CLAIMCLR bit assignments

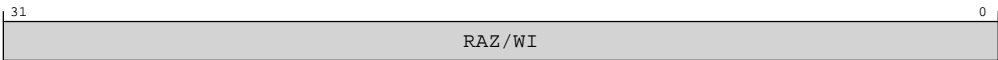


Table B-463: DBROM\_CLAIMCLR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
DBROM	0xFA4	None

This interface is accessible as follows:

RW

B.2.2.3.17 DBROM\_DEVAFF0, DebugBlock ROM table Device Affinity Register 0

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFA8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-232: EXT\_DBROM\_DEVAFF0 bit assignments

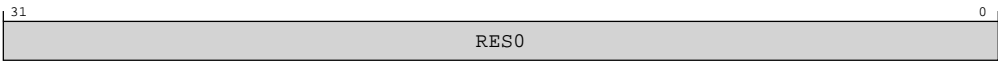


Table B-465: DBROM\_DEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFA8	None

This interface is accessible as follows:

RO

B.2.2.3.18 DBROM\_DEVAFF1, DebugBlock ROM table Device Affinity Register 1

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFAC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-233: EXT\_DBROM\_DEVAFF1 bit assignments

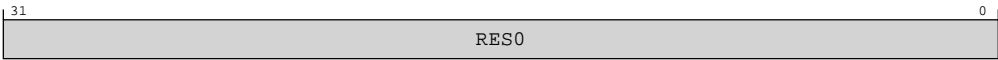


Table B-467: DBROM\_DEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFAC	None

This interface is accessible as follows:

RO

B.2.2.3.19 DBROM\_LAR, DebugBlock ROM table Software Lock Access Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFB0

Access type

RESERVEDW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-234: EXT\_DBROM\_LAR bit assignments



Table B-469: DBROM\_LAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
DBROM	0xFB0	None

This interface is accessible as follows:

WO

B.2.2.3.20 DBROM\_LSR, DebugBlock ROM table Software Lock Status Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFB4

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-235: EXT\_DBROM\_LSR bit assignments

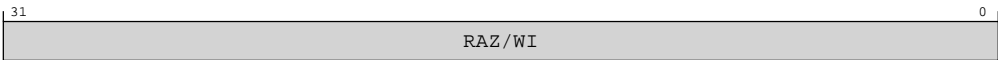


Table B-471: DBROM\_LSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
DBROM	0xFB4	None

This interface is accessible as follows:

RO

B.2.2.3.21 DBROM\_AUTHSTATUS, DebugBlock ROM table Authentication Status Register

Provides information about the state of the authentication interface for debug.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFB8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-236: EXT\_DBROM\_AUTHSTATUS bit assignments

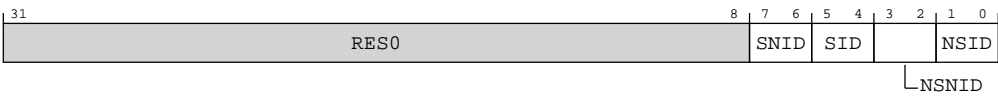


Table B-473: DBROM\_AUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure Non-invasive Debug.  ExternalSecureNoninvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx

Bits	Name	Description	Reset
[5:4]	SID	Secure Invasive Debug.  <b>0b10</b> Secure invasive debug disabled. ExternalSecureInvasiveDebugEnabled() == FALSE.  <b>0b11</b> Secure invasive debug enabled. ExternalSecureInvasiveDebugEnabled() == TRUE.	xx
[3:2]	NSNID	Non-secure Non-invasive Debug.  ExternalNoninvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx
[1:0]	NSID	Non-secure Invasive Debug.  ExternalInvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx

Accessibility

Component	Offset	Range
DBROM	0xFB8	None

This interface is accessible as follows:

RO

B.2.2.3.22 DBROM\_DEVARCH, DebugBlock ROM table Device Architecture Register

Identifies the architect and architecture of a CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFBC

Access type

RO

Reset value

0100 0111 0111 0000 0000 1010 1111 0111



Bit descriptions

Figure B-237: EXT\_DBROM\_DEVARCH bit assignments

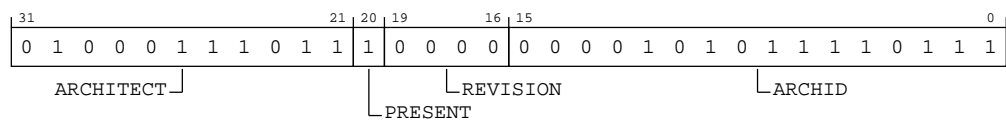


Table B-475: DBROM\_DEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect.  <b>0b01000111011</b> JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	Present.  <b>0b1</b> DEVARCH information present.	0b1
[19:16]	REVISION	Revision.  <b>0b0000</b> Revision 0.	0b0000
[15:0]	ARCHID	Architecture ID.  <b>0b0000101011110111</b> ROM Table v0. The debug tool must inspect ext-DBROM_DEVTYPE and ext-DBROM_DEVID to determine further information about the ROM Table.	0x0AF7

Accessibility

Component	Offset	Range
DBROM	0xFBC	None

This interface is accessible as follows:

RO

B.2.2.3.23 DBROM\_DEVID2, DebugBlock ROM table Device Configuration Register 2

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFC0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-238: EXT\_DBROM\_DEVID2 bit assignments

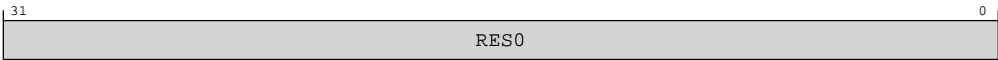


Table B-477: DBROM\_DEVID2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFC0	None

This interface is accessible as follows:

RO

B.2.2.3.24 DBROM\_DEVID1, DebugBlock ROM table Device Configuration Register 1

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width  
32

Component  
DBROM

Register offset  
0xFC4

Access type  
RO

Reset value

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

31

27

23

19

15

11

7

3

0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-239: EXT\_DBROM\_DEVID1 bit assignments

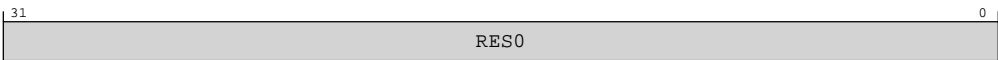


Table B-479: DBROM\_DEVID1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFC4	None

This interface is accessible as follows:

RO

B.2.2.3.25 DBROM\_DEVID, DebugBlock ROM table Device Configuration Register

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

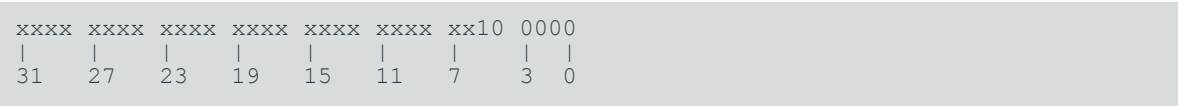
Register offset

0xFC8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-240: EXT\_DBROM\_DEVID bit assignments

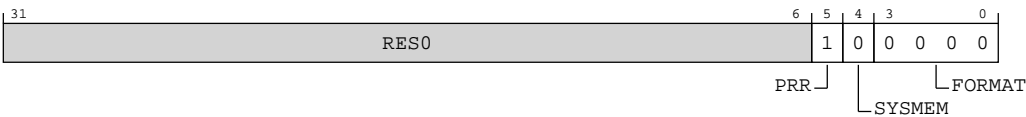


Table B-481: DBROM\_DEVID bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	PRR	Power Request functionality included.  0b1 Power Request functionality included. ext-DBROM_PRIDR0 is implemented.	0b1

Bits	Name	Description	Reset
[4]	SYSMEM	System memory present.  <b>0b0</b> System memory is not present on the bus.	0b0
[3:0]	FORMAT	ROM format.  <b>0b0000</b> 32-bit format 0.	0b0000

Accessibility

Component	Offset	Range
DBROM	0xFC8	None

This interface is accessible as follows:

RO

B.2.2.3.26 DBROM\_DEVTYPE, DebugBlock ROM table Device Type Register

A debugger can use DEVTYPE to obtain information about a component that has an unrecognized part number.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFCC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-241: EXT\_DBROM\_DEVTYPE bit assignments



Table B-483: DBROM\_DEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Sub number <b>0b0000</b> Other, undefined.	0b0000
[3:0]	MAJOR	Major number <b>0b0000</b> Miscellaneous.	0b0000

Accessibility

Component	Offset	Range
DBROM	0xFCC	None

This interface is accessible as follows:

RO

B.2.2.3.27 DBROM\_PIDR4, DebugBlock ROM table Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

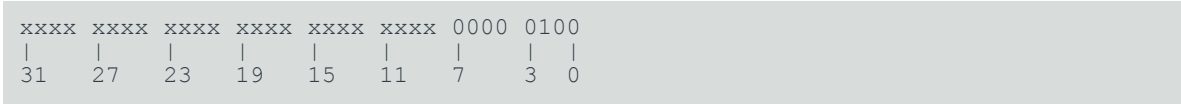
Register offset

0xFD0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-242: EXT\_DBROM\_PIDR4 bit assignments



Table B-485: DBROM\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count.  0b0000 The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code.  0b0100 Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
DBROM	0xFD0	None

This interface is accessible as follows:

RO

B.2.2.3.28 DBROM\_PIDR5, DebugBlock ROM table Peripheral Identification Register 5

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

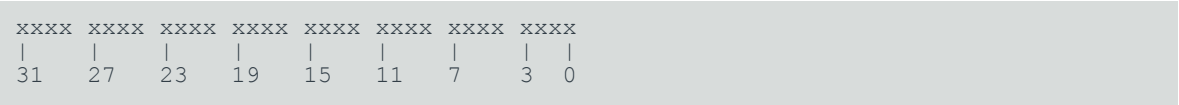
Register offset

0xFD4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-243: EXT\_DBROM\_PIDR5 bit assignments

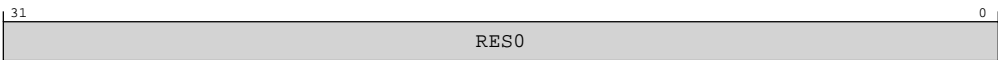


Table B-487: DBROM\_PIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFD4	None

This interface is accessible as follows:

RO



B.2.2.3.29 DBROM\_PIDR6, DebugBlock ROM table Peripheral Identification Register 6

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFD8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-244: EXT\_DBROM\_PIDR6 bit assignments

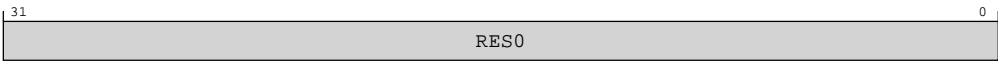


Table B-489: DBROM\_PIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFD8	None

This interface is accessible as follows:

RO

B.2.2.3.30 DBROM\_PIDR7, DebugBlock ROM table Peripheral Identification Register 7

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFDC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-245: EXT\_DBROM\_PIDR7 bit assignments

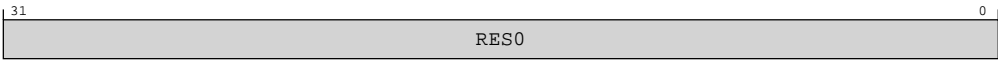


Table B-491: DBROM\_PIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
DBROM	0xFDC	None

This interface is accessible as follows:

RO

B.2.2.3.31 DBROM\_PIDR0, DebugBlock ROM table Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFE0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-246: EXT\_DBROM\_PIDR0 bit assignments

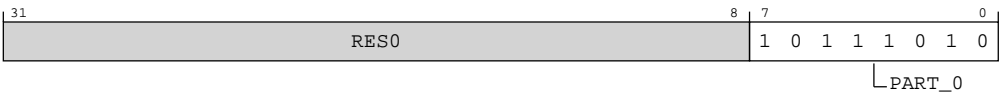


Table B-493: DBROM\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:0]	PART_0	Part number bits [7:0].  <b>0b10111010</b> Cortex-R82/Cortex-R82AE DebugBlock ROM table. Bits [7:0] of part number 0x4BA.	0xBA

Accessibility

Component	Offset	Range
DBROM	0xFE0	None

This interface is accessible as follows:

RO

B.2.2.3.32 DBROM\_PIDR1, DebugBlock ROM table Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFE4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-247: EXT\_DBROM\_PIDR1 bit assignments

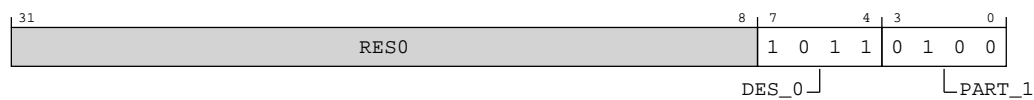


Table B-495: DBROM\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0]. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b0100</b> Cortex-R82/Cortex-R82AE DebugBlock ROM table. Bits [11:8] of part number 0x4BA.	0b0100

Accessibility

Component	Offset	Range
DBROM	0xFE4	None

This interface is accessible as follows:

RO

B.2.2.3.33 DBROM\_PIDR2, DebugBlock ROM table Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-248: EXT\_DBROM\_PIDR2 bit assignments

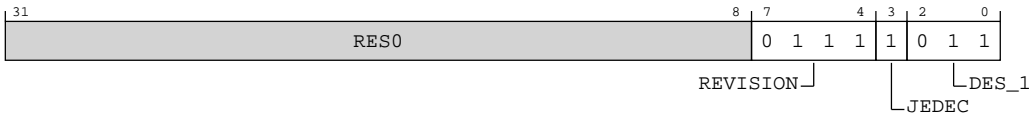


Table B-497: DBROM\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
DBROM	0xFE8	None

This interface is accessible as follows:

RO

B.2.2.3.34 DBROM\_PIDR3, DebugBlock ROM table Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFEC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-249: EXT\_DBROM\_PIDR3 bit assignments

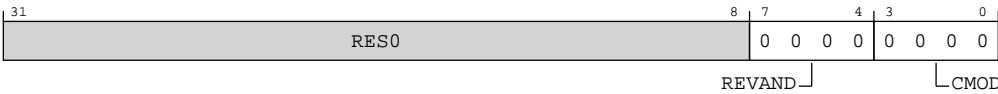


Table B-499: DBROM\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes. <b>0b0000</b> No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified. <b>0b0000</b> The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
DBROM	0xFEC	None

This interface is accessible as follows:

RO

B.2.2.3.35 DBROM\_CIDR0, DebugBlock ROM table Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFF0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	1101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-250: EXT\_DBROM\_CIDR0 bit assignments





Table B-501: DBROM\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble.  <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
DBROM	0xFF0	None

This interface is accessible as follows:

RO

B.2.2.3.36 DBROM\_CIDR1, DebugBlock ROM table Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

Register offset

0xFF4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-251: EXT\_DBROM\_CIDR1 bit assignments

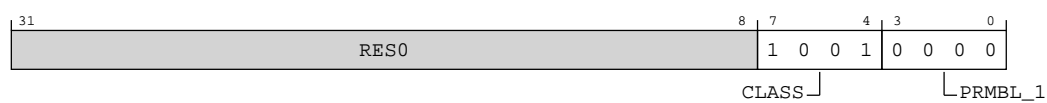


Table B-503: DBROM\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1001</b> CoreSight component.	0b1001
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
DBROM	0xFF4	None

This interface is accessible as follows:

RO

B.2.2.3.37 DBROM\_CIDR2, DebugBlock ROM table Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

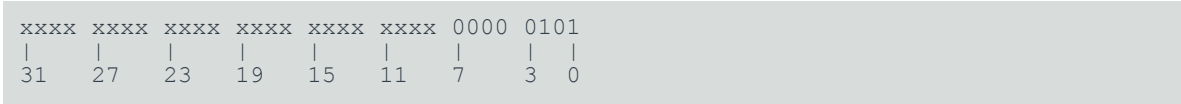
Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-252: EXT\_DBROM\_CIDR2 bit assignments



Table B-505: DBROM\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble. <b>0b000000101</b> CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
DBROM	0xFF8	None

This interface is accessible as follows:

RO

B.2.2.3.38 DBROM\_CIDR3, DebugBlock ROM table Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

DBROM

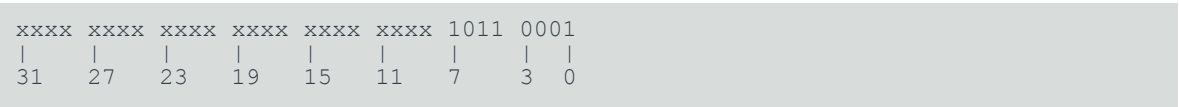
Register offset

0xFFC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-253: EXT\_DBROM\_CIDR3 bit assignments



Table B-507: DBROM\_CIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble. <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
DBROM	0xFFC	None

This interface is accessible as follows:

RO

B.2.2.4 External CLUSTERROM register description

This section includes the register descriptions for all memory-mapped CLUSTERROM registers that are accessed for the cluster.

B.2.2.4.1 CLUSTERROM\_ROMENTRY0, Cluster ROM table Entry 0

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x000

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x011
31	27	23	19	15	11	7	3 0

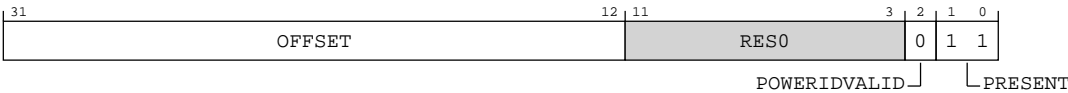


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-254: EXT\_CLUSTERROM\_ROMENTRY0 bit assignments



**Table B-509: CLUSTERROM\_ROMENTRY0 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000001</b> Cluster PMU at address 0x0_2000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000010000</b> Cluster PMU at address 0x21_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b> The ROM Entry is present.</p>	0b11

### Accessibility

Component	Offset	Range
CLUSTERROM	0x000	None

This interface is accessible as follows:

RO

#### B.2.2.4.2 CLUSTERROM\_ROMENTRY1, Cluster ROM table Entry 1

Provides the address offset for one CoreSight component.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

CLUSTERROM

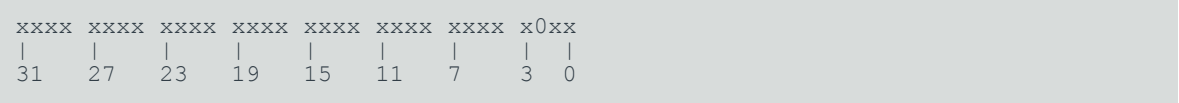
Register offset

0x004

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-255: EXT\_CLUSTERROM\_ROMENTRY1 bit assignments

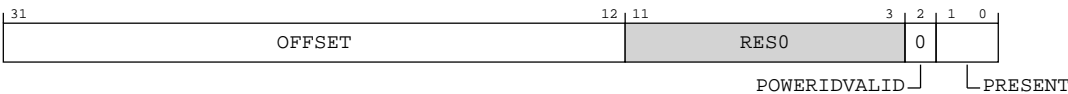


Table B-511: CLUSTERROM\_ROMENTRY1 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000010</b> Cluster ELA at address 0x0_3000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000000000100000</b> Cluster ELA at address 0x22_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b> A power domain ID is not provided.</p>	0b0

Bits	Name	Description	Reset
[1:0]	PRESENT	<b>When ELA == 1</b> Indicates whether an entry is present at this location in the ROM Table. <b>11</b> The ROM Entry is present.  <b>Otherwise</b> Indicates whether an entry is present at this location in the ROM Table. <b>10</b> The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.	xx

Accessibility

Component	Offset	Range
CLUSTERROM	0x004	None

This interface is accessible as follows:

RO

B.2.2.4.3 CLUSTERROM\_ROMENTRY2, Cluster ROM table Entry 2

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x008

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxx0	0000	x111
31	27	23	19	15	11	7	3 0





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-256: EXT\_CLUSTERROM\_ROMENTRY2 bit assignments

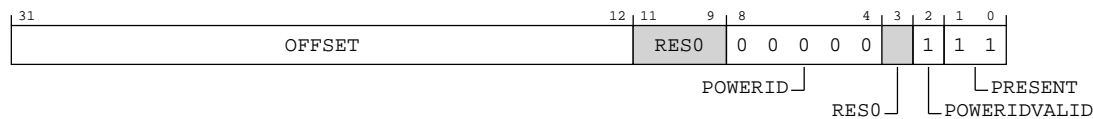


Table B-513: CLUSTERROM\_ROMENTRY2 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000000000000100</b> Core 0 ROM table at address 0x0_5000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000011000000000</b> Core 0 ROM table at address 0x80_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00000</b> PDCPU0 power domain.	0b00000
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table. <b>0b11</b> The ROM Entry is present.	0b11

Accessibility

Component	Offset	Range
CLUSTERROM	0x008	None

This interface is accessible as follows:

RO

B.2.2.4.4 CLUSTERROM\_ROMENTRY3, Cluster ROM table Entry 3

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x00C

Access type

RO

Reset value

When NUM\_CORES >= 2

xxxx xxxx xxxx xxxx xxxx xxx0 0001 x1xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

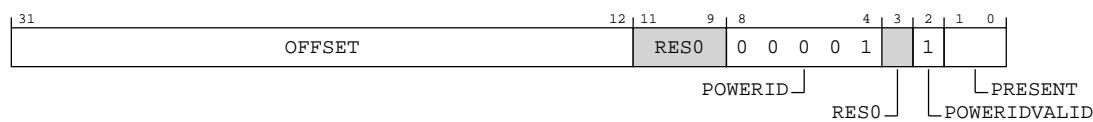


Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 2

Figure B-257: EXT\_CLUSTERROM\_ROMENTRY3 bit assignments



**Table B-515: CLUSTERROM\_ROMENTRY3 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000001010</b> Core 1 ROM table at address 0x0_B000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000011100000000</b> Core 1 ROM table at address 0x90_0000.</p>	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	<p>The power domain ID of the component.</p> <p><b>0b00001</b> PDCPU1 power domain.</p>	0b00001
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b1</b> The POWERID field provides a power domain ID.</p>	0b1
[1:0]	PRESENT	<p><b>When CFGCEMODE == 3</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>10</b> The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.</p> <p><b>Otherwise</b></p> <p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>11</b> The ROM Entry is present.</p>	xx

**Figure B-258: EXT\_CLUSTERROM\_ROMENTRY3 bit assignments****Table B-516: CLUSTERROM\_ROMENTRY3 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x00C	None

This interface is accessible as follows:

RO

B.2.2.4.5 CLUSTERROM\_ROMENTRY4, Cluster ROM table Entry 4

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x010

Access type

RO

Reset value

When NUM\_CORES >= 3

xxxx xxxx xxxx xxxx xxxx xxx0 0010 x111  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 3

Figure B-259: EXT\_CLUSTERROM\_ROMENTRY4 bit assignments

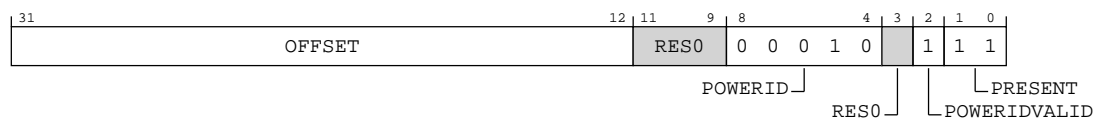


Table B-518: CLUSTERROM\_ROMENTRY4 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000000000000010000</b> Core 2 ROM table at address 0x1_1000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>0000000001000000000000</b> Core 2 ROM table at address 0xA0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00010</b> PDCPU2 power domain.	0b00010
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table. <b>0b11</b> The ROM Entry is present.	0b11

Figure B-260: EXT\_CLUSTERROM\_ROMENTRY4 bit assignments



Table B-519: CLUSTERROM\_ROMENTRY4 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x010	None

This interface is accessible as follows:

RO

B.2.2.4.6 CLUSTERROM\_ROMENTRY5, Cluster ROM table Entry 5

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x014

Access type

RO

Reset value

When NUM\_CORES >= 4

xxxx xxxx xxxx xxxx xxxx xxx0 0011 x1xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 4

Figure B-261: EXT\_CLUSTERROM\_ROMENTRY5 bit assignments

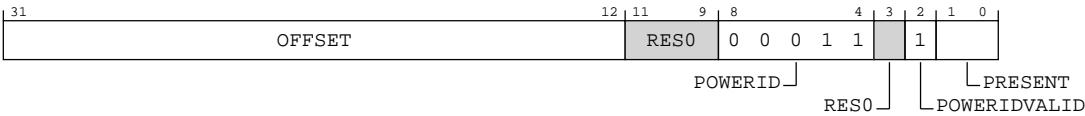


Table B-521: CLUSTERROM\_ROMENTRY5 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>000000000000000010110</b> Core 3 ROM table at address 0x1_7000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000100100000000</b> Core 3 ROM table at address 0xB0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00011</b> PDCPU3 power domain.	0b00011
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	<b>When CFGCEMODE == 3</b> Indicates whether an entry is present at this location in the ROM Table. <b>10</b> The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.  <b>Otherwise</b> Indicates whether an entry is present at this location in the ROM Table. <b>11</b> The ROM Entry is present.	xx

Figure B-262: EXT\_CLUSTERROM\_ROMENTRY5 bit assignments

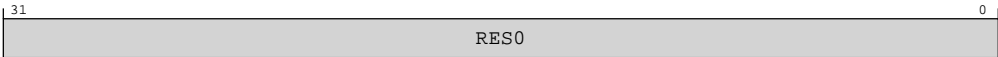


Table B-522: CLUSTERROM\_ROMENTRY5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x014	None

This interface is accessible as follows:

RO

B.2.2.4.7 CLUSTERROM\_ROMENTRY6, Cluster ROM table Entry 6

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x018

Access type

RO

Reset value

When NUM\_CORES >= 5

xxxx xxxx xxxx xxxx xxxx xxx0 0100 x111

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 5



Figure B-263: EXT\_CLUSTERROM\_ROMENTRY6 bit assignments

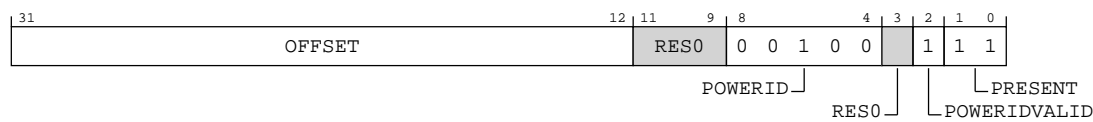


Table B-524: CLUSTERROM\_ROMENTRY6 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>000000000000000011100</b> Core 4 ROM table at address 0x1_D000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000101000000000</b> Core 4 ROM table at address 0xC0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00100</b> PDCPU4 power domain.	0b00100
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table. <b>0b11</b> The ROM Entry is present.	0b11

Figure B-264: EXT\_CLUSTERROM\_ROMENTRY6 bit assignments



Table B-525: CLUSTERROM\_ROMENTRY6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x018	None

This interface is accessible as follows:

RO

B.2.2.4.8 CLUSTERROM\_ROMENTRY7, Cluster ROM table Entry 7

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x01C

Access type

RO

Reset value

When NUM\_CORES >= 6

xxxx xxxx xxxx xxxx xxxx xxx0 0101 x1xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 6

Figure B-265: EXT\_CLUSTERROM\_ROMENTRY7 bit assignments

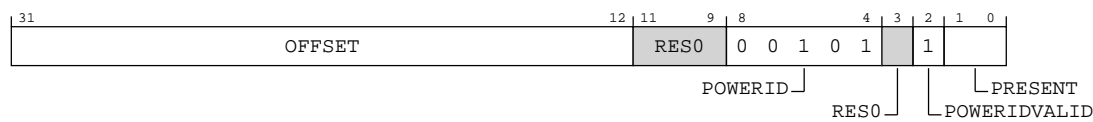


Table B-527: CLUSTERROM\_ROMENTRY7 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000000000100010</b> Core 5 ROM table at address 0x2_3000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000101100000000</b> Core 5 ROM table at address 0xD0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00101</b> PDCPU5 power domain.	0b00101
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	<b>When CFGCEMODE == 3</b> Indicates whether an entry is present at this location in the ROM Table. <b>10</b> The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.  <b>Otherwise</b> Indicates whether an entry is present at this location in the ROM Table. <b>11</b> The ROM Entry is present.	xx

Figure B-266: EXT\_CLUSTERROM\_ROMENTRY7 bit assignments

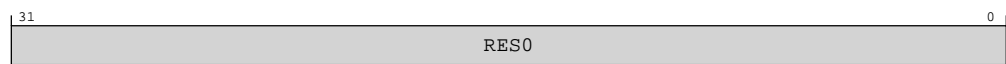


Table B-528: CLUSTERROM\_ROMENTRY7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x01C	None

This interface is accessible as follows:

RO

B.2.2.4.9 CLUSTERROM\_ROMENTRY8, Cluster ROM table Entry 8

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x020

Access type

RO

Reset value

When NUM\_CORES >= 7

xxxx xxxx xxxx xxxx xxxx xxx0 0110 x111

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 7

Figure B-267: EXT\_CLUSTERROM\_ROMENTRY8 bit assignments

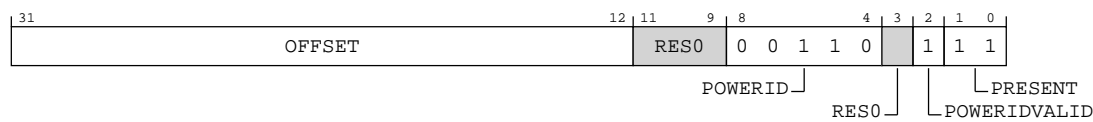


Table B-530: CLUSTERROM\_ROMENTRY8 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000000000101000</b> Core 6 ROM table at address 0x2_9000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000110000000000</b> Core 6 ROM table at address 0xE0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00110</b> PDCPU6 power domain.	0b00110
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table. <b>0b11</b> The ROM Entry is present.	0b11

Figure B-268: EXT\_CLUSTERROM\_ROMENTRY8 bit assignments



Table B-531: CLUSTERROM\_ROMENTRY8 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x020	None

This interface is accessible as follows:

RO

B.2.2.4.10 CLUSTERROM\_ROMENTRY9, Cluster ROM table Entry 9

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0x024

Access type

RO

Reset value

When NUM\_CORES == 8

xxxx xxxx xxxx xxxx xxxx xxx0 0111 x1xx  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES == 8

Figure B-269: EXT\_CLUSTERROM\_ROMENTRY9 bit assignments

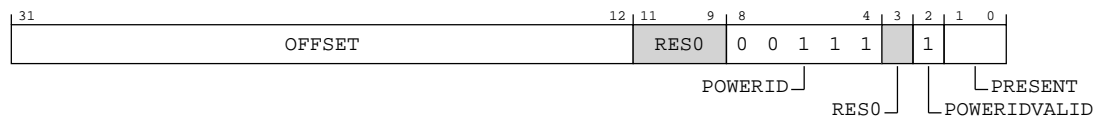


Table B-533: CLUSTERROM\_ROMENTRY9 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<b>When DENSE_CS_ADDR_MAP == 1</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000000000101110</b> Core 7 ROM table at address 0x2_F000.  <b>Otherwise</b> The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET << 12). <b>00000000110100000000</b> Core 7 ROM table at address 0xF0_0000.	20{x}
[11:9]	RES0	Reserved	RES0
[8:4]	POWERID	The power domain ID of the component. <b>0b00111</b> PDCPU7 power domain.	0b00111
[3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID. <b>0b1</b> The POWERID field provides a power domain ID.	0b1
[1:0]	PRESENT	<b>When CFGCEMODE == 3</b> Indicates whether an entry is present at this location in the ROM Table. <b>10</b> The ROM Entry is not present, but this ROM Entry is not the final one in the ROM Table.  <b>Otherwise</b> Indicates whether an entry is present at this location in the ROM Table. <b>11</b> The ROM Entry is present.	xx

Figure B-270: EXT\_CLUSTERROM\_ROMENTRY9 bit assignments

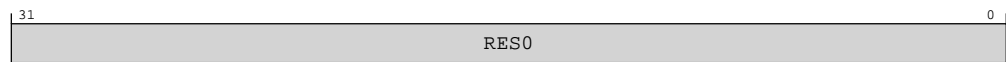


Table B-534: CLUSTERROM\_ROMENTRY9 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0x024	None

This interface is accessible as follows:

RO

B.2.2.4.11 CLUSTERROM\_DBGPCRO, Cluster ROM table Debug Power Control Register 0

Controls power requests for PDCPU0.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA00

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxx1
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure B-271: EXT\_CLUSTERROM\_DBGPCR0 bit assignments

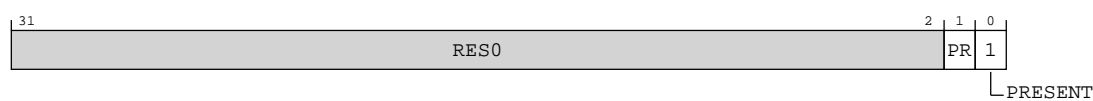


Table B-536: CLUSTERROM\_DBGPCR0 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  0b0 Power is not requested for PDCPU0.  0b1 Power is requested for PDCPU0.	x
[0]	PRESENT	Power request implemented.  0b1 Power request for PDCPU0 is implemented.	0b1

Accessibility

Component	Offset	Range
CLUSTERROM	0xA00	None

This interface is accessible as follows:

RW

B.2.2.4.12 CLUSTERROM\_DBGPCR1, Cluster ROM table Debug Power Control Register 1

Controls power requests for PDCPU1.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA04

Access type

RW

Reset value

When NUM\_CORES >= 2

XXXX XXXX XXXX XXXX XXXX XXXX XXX1  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 2

Figure B-272: EXT\_CLUSTERROM\_DBGPCR1 bit assignments



Table B-538: CLUSTERROM\_DBGPCR1 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  0b0 Power is not requested for PDCPU1.  0b1 Power is requested for PDCPU1.	x
[0]	PRESENT	Power request implemented.  0b1 Power request for PDCPU1 is implemented.	0b1

Figure B-273: EXT\_CLUSTERROM\_DBGPCR1 bit assignments

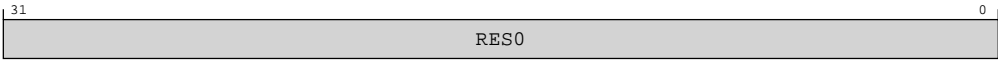


Table B-539: CLUSTERROM\_DBGPCR1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA04	None

This interface is accessible as follows:

RW

B.2.2.4.13 CLUSTERROM\_DBGPCR2, Cluster ROM table Debug Power Control Register 2

Controls power requests for PDCPU2.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA08

Access type

RW

Reset value

When NUM\_CORES >= 3

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxx1  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 3

Figure B-274: EXT\_CLUSTERROM\_DBGPCR2 bit assignments

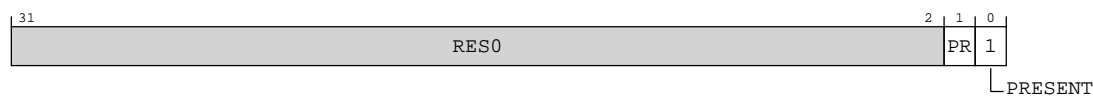


Table B-541: CLUSTERROM\_DBGPCR2 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  0b0 Power is not requested for PDCPU2.  0b1 Power is requested for PDCPU2.	x
[0]	PRESENT	Power request implemented.  0b1 Power request for PDCPU2 is implemented.	0b1

Figure B-275: EXT\_CLUSTERROM\_DBGPCR2 bit assignments

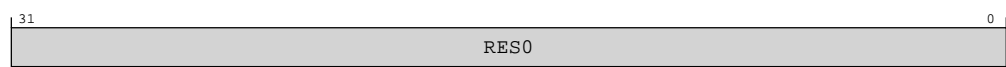


Table B-542: CLUSTERROM\_DBGPCR2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA08	None

This interface is accessible as follows:

RW

B.2.2.4.14 CLUSTERROM\_DBGPCR3, Cluster ROM table Debug Power Control Register 3

Controls power requests for PDCPU3.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA0C

Access type

RW

Reset value

When NUM\_CORES >= 4

xxxx xxxx xxxx xxxx xxxx xxxx xxx1  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 4

Figure B-276: EXT\_CLUSTERROM\_DBGPCR3 bit assignments

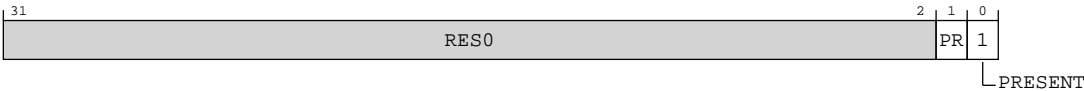


Table B-544: CLUSTERROM\_DBGPCR3 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  <b>0b0</b> Power is not requested for PDCPU3.  <b>0b1</b> Power is requested for PDCPU3.	x
[0]	PRESENT	Power request implemented.  <b>0b1</b> Power request for PDCPU3 is implemented.	0b1

Figure B-277: EXT\_CLUSTERROM\_DBGPCR3 bit assignments

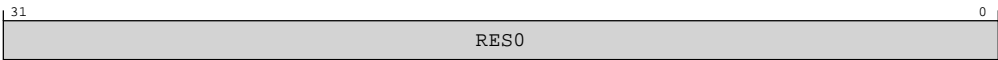


Table B-545: CLUSTERROM\_DBGPCR3 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA0C	None

This interface is accessible as follows:

RW

B.2.2.4.15 CLUSTERROM\_DBGPCR4, Cluster ROM table Debug Power Control Register 4

Controls power requests for PDCPU4.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA10

Access type

RW

Reset value

When NUM\_CORES >= 5

xxxx xxxx xxxx xxxx xxxx xxxx xxx1  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 5

Figure B-278: EXT\_CLUSTERROM\_DBGPCR4 bit assignments

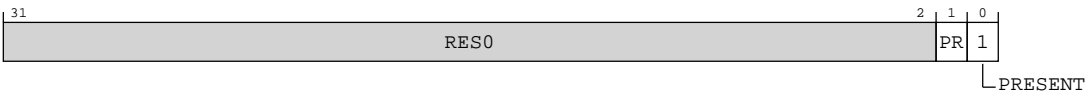


Table B-547: CLUSTERROM\_DBGPCR4 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  0b0 Power is not requested for PDCPU4.  0b1 Power is requested for PDCPU4.	x
[0]	PRESENT	Power request implemented.  0b1 Power request for PDCPU4 is implemented.	0b1

Figure B-279: EXT\_CLUSTERROM\_DBGPCR4 bit assignments

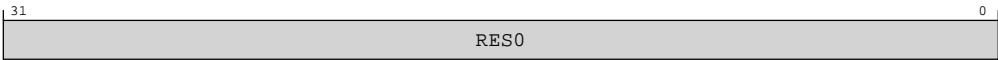


Table B-548: CLUSTERROM\_DBGPCR4 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA10	None

This interface is accessible as follows:

RW

B.2.2.4.16 CLUSTERROM\_DBGPCR5, Cluster ROM table Debug Power Control Register 5

Controls power requests for PDCPU5.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA14

Access type

RW

Reset value

When NUM\_CORES >= 6

xxxx xxxx xxxx xxxx xxxx xxxx xxx1  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 6

Figure B-280: EXT\_CLUSTERROM\_DBGPCR5 bit assignments

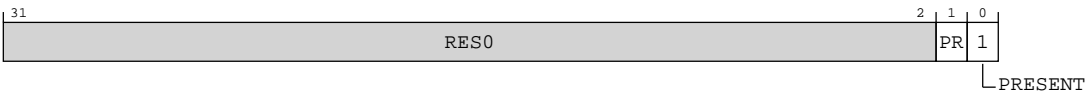


Table B-550: CLUSTERROM\_DBGPCR5 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[1]	PR	Power Request.  <b>0b0</b> Power is not requested for PDCPU5.  <b>0b1</b> Power is requested for PDCPU5.	x
[0]	PRESENT	Power request implemented.  <b>0b1</b> Power request for PDCPU5 is implemented.	0b1

Figure B-281: EXT\_CLUSTERROM\_DBGPCR5 bit assignments

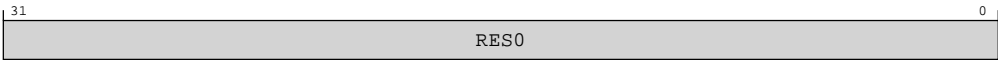


Table B-551: CLUSTERROM\_DBGPCR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA14	None

This interface is accessible as follows:

RW

B.2.2.4.17 CLUSTERROM\_DBGPCR6, Cluster ROM table Debug Power Control Register 6

Controls power requests for PDCPU6.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA18

Access type  
RW

Reset value

When NUM\_CORES >= 7

XXXX XXXX XXXX XXXX XXXX XXXX XXX1

XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 7

Figure B-282: EXT\_CLUSTERROM\_DBGPCR6 bit assignments

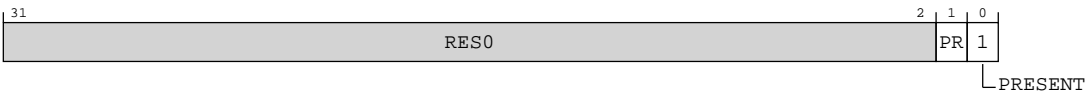


Table B-553: CLUSTERROM\_DBGPCR6 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request. <b>0b0</b> Power is not requested for PDCPU6. <b>0b1</b> Power is requested for PDCPU6.	x
[0]	PRESENT	Power request implemented. <b>0b1</b> Power request for PDCPU6 is implemented.	0b1

Figure B-283: EXT\_CLUSTERROM\_DBGPCR6 bit assignments

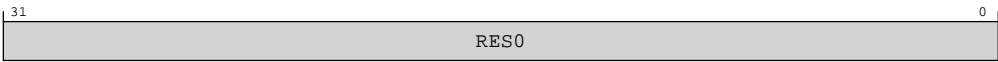


Table B-554: CLUSTERROM\_DBGPCR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA18	None

This interface is accessible as follows:

RW

B.2.2.4.18 CLUSTERROM\_DBGPCR7, Cluster ROM table Debug Power Control Register 7

Controls power requests for PDCPU7.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA1C

Access type

RW

Reset value

When NUM\_CORES == 8

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxx1  
xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES == 8

Figure B-284: EXT\_CLUSTERROM\_DBGPCR7 bit assignments

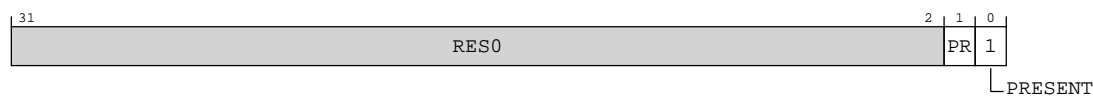


Table B-556: CLUSTERROM\_DBGPCR7 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PR	Power Request.  0b0 Power is not requested for PDCPU7.  0b1 Power is requested for PDCPU7.	x
[0]	PRESENT	Power request implemented.  0b1 Power request for PDCPU7 is implemented.	0b1

Figure B-285: EXT\_CLUSTERROM\_DBGPCR7 bit assignments

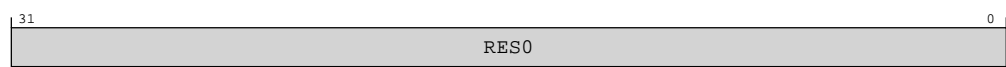


Table B-557: CLUSTERROM\_DBGPCR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA1C	None

This interface is accessible as follows:

RW

B.2.2.4.19 CLUSTERROM\_DBGPSR0, Cluster ROM table Debug Power Status Register 0

Indicates the power status for PDCPU0.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA80

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-286: EXT\_CLUSTERROM\_DBGPSR0 bit assignments

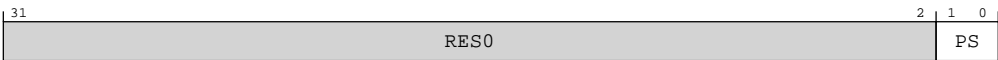


Table B-559: CLUSTERROM\_DBGPSR0 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU0 might not be powered.  <b>0b01</b> PDCPU0 is powered.	xx

Accessibility

Component	Offset	Range
CLUSTERROM	0xA80	None

This interface is accessible as follows:

RO

B.2.2.4.20 CLUSTERROM\_DBGPSR1, Cluster ROM table Debug Power Status Register 1

Indicates the power status for PDCPU1.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA84

Access type

RO

Reset value

When NUM\_CORES >= 2

XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 2

Figure B-287: EXT\_CLUSTERROM\_DBGPSR1 bit assignments

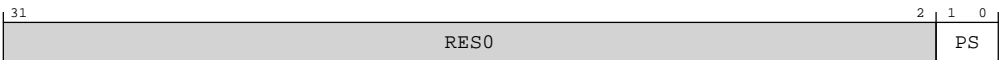


Table B-561: CLUSTERROM\_DBGPSR1 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU1 might not be powered.  <b>0b01</b> PDCPU1 is powered.	xx

Figure B-288: EXT\_CLUSTERROM\_DBGPSR1 bit assignments

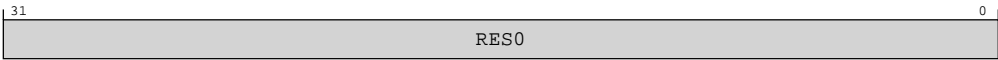


Table B-562: CLUSTERROM\_DBGPSR1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA84	None

This interface is accessible as follows:

RO

B.2.2.4.21 CLUSTERROM\_DBGPSR2, Cluster ROM table Debug Power Status Register 2

Indicates the power status for PDCPU2.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA88

Access type

RO

Reset value

When NUM\_CORES >= 3

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 3

Figure B-289: EXT\_CLUSTERROM\_DBGPSR2 bit assignments

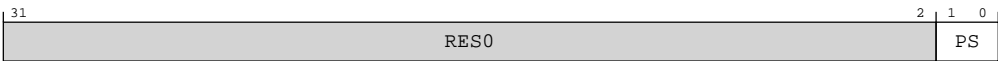


Table B-564: CLUSTERROM\_DBGPSR2 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1:0]	PS	Power Status.  0b00 PDCPU2 might not be powered.  0b01 PDCPU2 is powered.	xx

Figure B-290: EXT\_CLUSTERROM\_DBGPSR2 bit assignments



Table B-565: CLUSTERROM\_DBGPSR2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA88	None

This interface is accessible as follows:



RO

B.2.2.4.22 CLUSTERROM\_DBGPSR3, Cluster ROM table Debug Power Status Register 3

Indicates the power status for PDCPU3.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA8C

Access type

RO

Reset value

When NUM\_CORES >= 4

XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 4

Figure B-291: EXT\_CLUSTERROM\_DBGPSR3 bit assignments

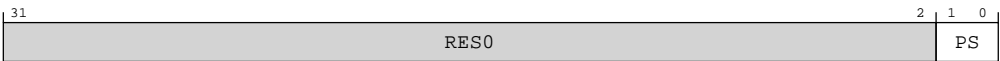


Table B-567: CLUSTERROM\_DBGPSR3 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU3 might not be powered.  <b>0b01</b> PDCPU3 is powered.	xx

Figure B-292: EXT\_CLUSTERROM\_DBGPSR3 bit assignments

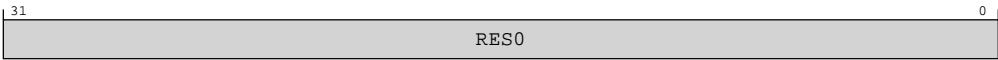


Table B-568: CLUSTERROM\_DBGPSR3 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA8C	None

This interface is accessible as follows:

RO

B.2.2.4.23 CLUSTERROM\_DBGPSR4, Cluster ROM table Debug Power Status Register 4

Indicates the power status for PDCPU4.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA90

Access type

RO

Reset value

When NUM\_CORES >= 5

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 5

Figure B-293: EXT\_CLUSTERROM\_DBGPSR4 bit assignments

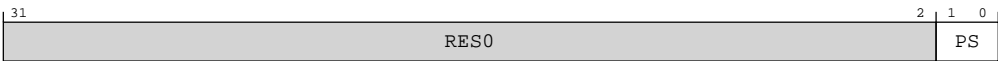


Table B-570: CLUSTERROM\_DBGPSR4 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU4 might not be powered.  <b>0b01</b> PDCPU4 is powered.	xx

Figure B-294: EXT\_CLUSTERROM\_DBGPSR4 bit assignments

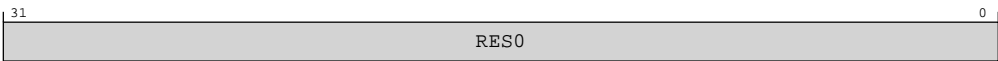


Table B-571: CLUSTERROM\_DBGPSR4 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA90	None

This interface is accessible as follows:

RO

B.2.2.4.24 CLUSTERROM\_DBGPSR5, Cluster ROM table Debug Power Status Register 5

Indicates the power status for PDCPU5.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA94

Access type

RO

Reset value

When NUM\_CORES >= 6

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 6

Figure B-295: EXT\_CLUSTERROM\_DBGPSR5 bit assignments

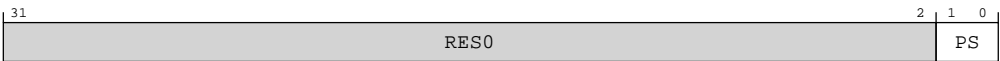


Table B-573: CLUSTERROM\_DBGPSR5 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU5 might not be powered.  <b>0b01</b> PDCPU5 is powered.	xx

Figure B-296: EXT\_CLUSTERROM\_DBGPSR5 bit assignments

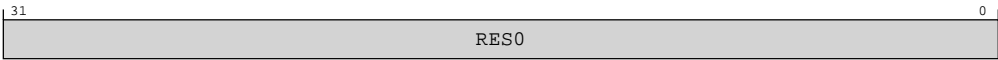


Table B-574: CLUSTERROM\_DBGPSR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA94	None

This interface is accessible as follows:

RO

B.2.2.4.25 CLUSTERROM\_DBGPSR6, Cluster ROM table Debug Power Status Register 6

Indicates the power status for PDCPU6.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA98

Access type

RO

Reset value

When NUM\_CORES >= 7

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES >= 7

Figure B-297: EXT\_CLUSTERROM\_DBGPSR6 bit assignments

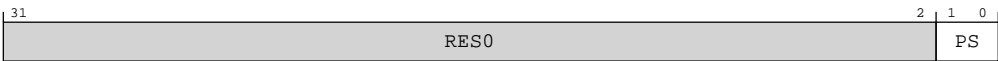


Table B-576: CLUSTERROM\_DBGPSR6 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU6 might not be powered.  <b>0b01</b> PDCPU6 is powered.	xx

Figure B-298: EXT\_CLUSTERROM\_DBGPSR6 bit assignments



Table B-577: CLUSTERROM\_DBGPSR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA98	None

This interface is accessible as follows:

RO

B.2.2.4.26 CLUSTERROM\_DBGPSR7, Cluster ROM table Debug Power Status Register 7

Indicates the power status for PDCPU7.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xA9C

Access type

RO

Reset value

When NUM\_CORES == 8

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX  
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When NUM\_CORES == 8

Figure B-299: EXT\_CLUSTERROM\_DBGPSR7 bit assignments

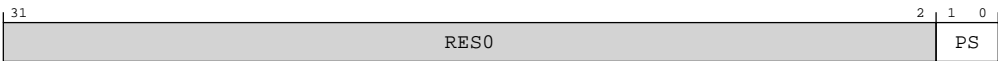


Table B-579: CLUSTERROM\_DBGPSR7 bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[1:0]	PS	Power Status.  <b>0b00</b> PDCPU7 might not be powered.  <b>0b01</b> PDCPU7 is powered.	xx

Figure B-300: EXT\_CLUSTERROM\_DBGPSR7 bit assignments

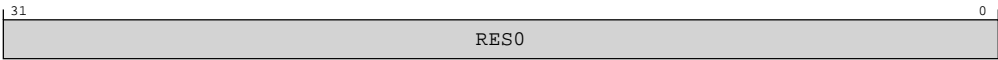


Table B-580: CLUSTERROM\_DBGPSR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xA9C	None

This interface is accessible as follows:

RO

B.2.2.4.27 CLUSTERROM\_PRIDR0, Cluster ROM table Power Request ID Register 0

Indicates the features of the power request functionality.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xC00

Access type

RO

Reset value







Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-301: EXT\_CLUSTERROM\_PRIDR0 bit assignments

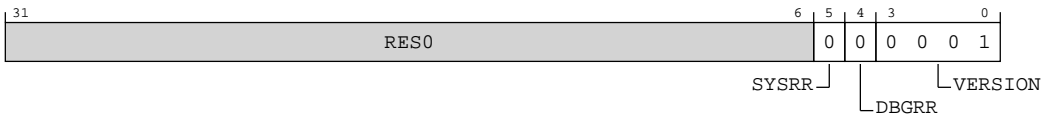


Table B-582: CLUSTERROM\_PRIDR0 bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	SYSRR	System reset request functionality present.  0b0 The system reset request functionality is not implemented.	0b0
[4]	DBGRR	Debug reset request functionality present.  0b0 The debug reset request functionality is not implemented.	0b0
[3:0]	VERSION	Version of the power request functionality.  0b0001 The power request functionality version 0, and the per-core controls for power requests (e.g. ext-CLUSTERROM_DBGPCR0 and ext-CLUSTERROM_DBGPSR0), are implemented.	0b0001

Accessibility

Component	Offset	Range
CLUSTERROM	0xC00	None

This interface is accessible as follows:

RO

B.2.2.4.28 CLUSTERROM\_ITCTRL, Cluster ROM table Integration Mode Control Register

No functional/integration mode switching implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

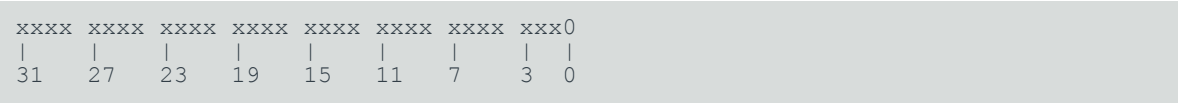
Register offset

0xF00

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-302: EXT\_CLUSTERROM\_ITCTRL bit assignments

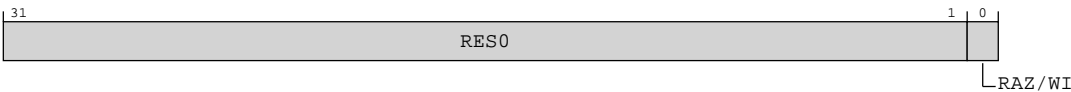


Table B-584: CLUSTERROM\_ITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERROM	0xF00	None

This interface is accessible as follows:

RW

B.2.2.4.29 CLUSTERROM\_CLAIMSET, Cluster ROM table Claim Tag Set Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFA0

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-303: EXT\_CLUSTERROM\_CLAIMSET bit assignments

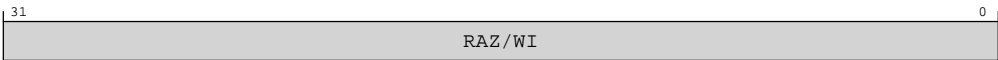


Table B-586: CLUSTERROM\_CLAIMSET bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERROM	0xFA0	None

This interface is accessible as follows:

RW

B.2.2.4.30 CLUSTERROM\_CLAIMCLR, Cluster ROM table Claim Tag Clear Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFA4

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-304: EXT\_CLUSTERROM\_CLAIMCLR bit assignments

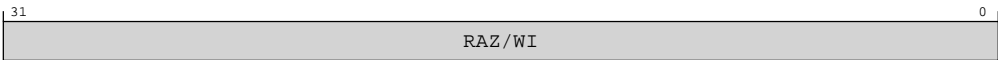


Table B-588: CLUSTERROM\_CLAIMCLR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERROM	0xFA4	None

This interface is accessible as follows:

RW

B.2.2.4.31 CLUSTERROM\_DEVAFF0, Cluster ROM table Device Affinity Register 0

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFA8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-305: EXT\_CLUSTERROM\_DEVAFF0 bit assignments

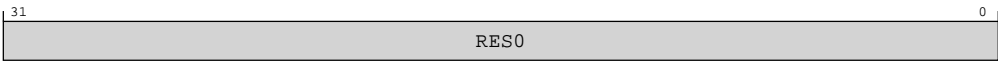


Table B-590: CLUSTERROM\_DEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFA8	None

This interface is accessible as follows:

RO

B.2.2.4.32 CLUSTERROM\_DEVAFF1, Cluster ROM table Device Affinity Register 1

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFAC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-306: EXT\_CLUSTERROM\_DEVAFF1 bit assignments

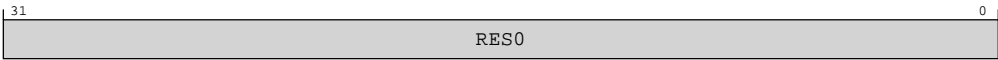


Table B-592: CLUSTERROM\_DEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFAC	None

This interface is accessible as follows:

RO

B.2.2.4.33 CLUSTERROM\_LAR, Cluster ROM table Software Lock Access Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFB0

Access type

RESERVEDW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-307: EXT\_CLUSTERROM\_LAR bit assignments



Table B-594: CLUSTERROM\_LAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERROM	0xFB0	None

This interface is accessible as follows:

WO

B.2.2.4.34 CLUSTERROM\_LSR, Cluster ROM table Software Lock Status Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFB4

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-308: EXT\_CLUSTERROM\_LSR bit assignments

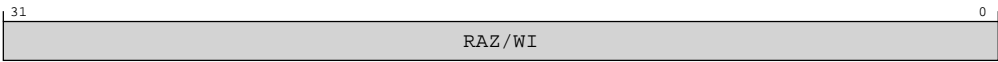


Table B-596: CLUSTERROM\_LSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
CLUSTERROM	0xFB4	None

This interface is accessible as follows:

RO



B.2.2.4.35 CLUSTERROM\_AUTHSTATUS, Cluster ROM table Authentication Status Register

Provides information about the state of the authentication interface for debug.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFB8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-309: EXT\_CLUSTERROM\_AUTHSTATUS bit assignments

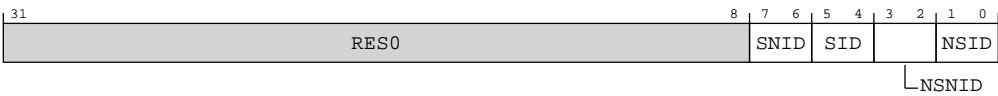


Table B-598: CLUSTERROM\_AUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure Non-invasive Debug.  ExternalSecureNoninvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx

Bits	Name	Description	Reset
[5:4]	SID	Secure Invasive Debug.  <b>0b10</b> Secure invasive debug disabled. ExternalSecureInvasiveDebugEnabled() == FALSE.  <b>0b11</b> Secure invasive debug enabled. ExternalSecureInvasiveDebugEnabled() == TRUE.	xx
[3:2]	NSNID	Non-secure Non-invasive Debug.  ExternalNoninvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx
[1:0]	NSID	Non-secure Invasive Debug.  ExternalInvasiveDebugEnabled() == ExternalSecureInvasiveDebugEnabled().  This field has the same value as the SID field.	xx

Accessibility

Component	Offset	Range
CLUSTERROM	0xFB8	None

This interface is accessible as follows:

RO

B.2.2.4.36 CLUSTERROM\_DEVARCH, Cluster ROM table Device Architecture Register

Identifies the architect and architecture of a CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFBC

Access type

RO

Reset value

0100 0111 0111 0000 0000 1010 1111 0111

Bit descriptions

Figure B-310: EXT\_CLUSTERROM\_DEVARCH bit assignments

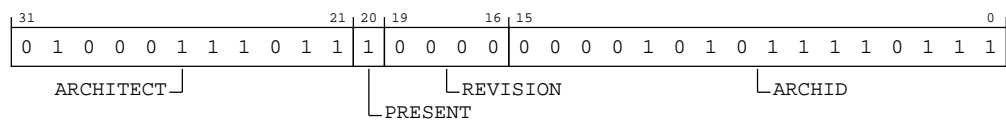


Table B-600: CLUSTERROM\_DEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect.  0b01000111011 JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	Present.  0b1 DEVARCH information present.	0b1
[19:16]	REVISION	Revision.  0b0000 Revision 0.	0b0000
[15:0]	ARCHID	Architecture ID.  0b0000101011110111 ROM Table v0. The debug tool must inspect ext-CLUSTERROM_DEVTYPE and ext-CLUSTERROM_DEVID to determine further information about the ROM Table.	0x0AF7

Accessibility

Component	Offset	Range
CLUSTERROM	0xFBC	None

This interface is accessible as follows:

RO

B.2.2.4.37 CLUSTERROM\_DEVID2, Cluster ROM table Device Configuration Register 2

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFC0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-311: EXT\_CLUSTERROM\_DEVID2 bit assignments

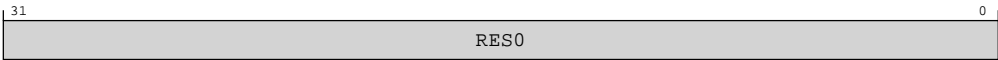


Table B-602: CLUSTERROM\_DEVID2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFC0	None

This interface is accessible as follows:

RO

B.2.2.4.38 CLUSTERROM\_DEVID1, Cluster ROM table Device Configuration Register 1

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

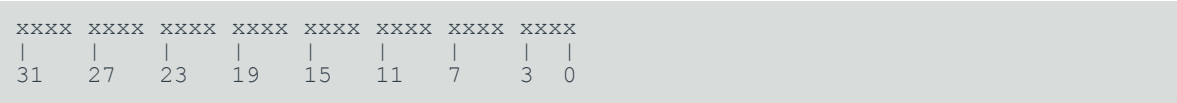
Register offset

0xFC4

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-312: EXT\_CLUSTERROM\_DEVID1 bit assignments

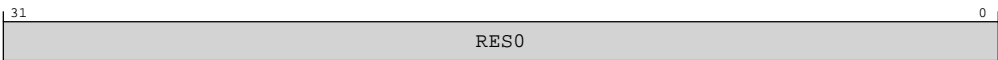


Table B-604: CLUSTERROM\_DEVID1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFC4	None

This interface is accessible as follows:

RO

B.2.2.4.39 CLUSTERROM\_DEVID, Cluster ROM table Device Configuration Register

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFC8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-313: EXT\_CLUSTERROM\_DEVID bit assignments

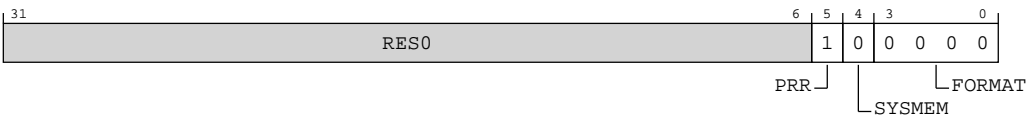


Table B-606: CLUSTERROM\_DEVID bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	PRR	Power Request functionality included.  0b1  Power Request functionality included. ext-CLUSTERROM_PRIDR0 is implemented.	0b1

Bits	Name	Description	Reset
[4]	SYSMEM	System memory present.  <b>0b0</b> System memory is not present on the bus.	0b0
[3:0]	FORMAT	ROM format.  <b>0b0000</b> 32-bit format 0.	0b0000

Accessibility

Component	Offset	Range
CLUSTERROM	0xFC8	None

This interface is accessible as follows:

RO

B.2.2.4.40 CLUSTERROM\_DEVTYPE, Cluster ROM table Device Type Register

A debugger can use DEVTYPE to obtain information about a component that has an unrecognized part number.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFCC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-314: EXT\_CLUSTERROM\_DEVTYPE bit assignments

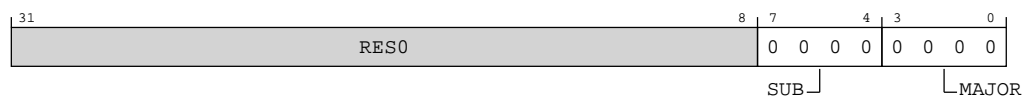


Table B-608: CLUSTERROM\_DEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Sub number <b>0b0000</b> Other, undefined.	0b0000
[3:0]	MAJOR	Major number <b>0b0000</b> Miscellaneous.	0b0000

Accessibility

Component	Offset	Range
CLUSTERROM	0xFCC	None

This interface is accessible as follows:

RO

B.2.2.4.41 CLUSTERROM\_PIDR4, Cluster ROM table Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

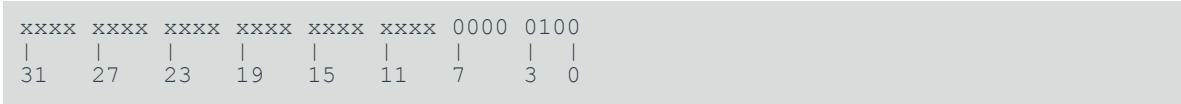
0xFD0

Access type

RO



Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-315: EXT\_CLUSTERROM\_PIDR4 bit assignments



Table B-610: CLUSTERROM\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count. <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code. <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
CLUSTERROM	0xFD0	None

This interface is accessible as follows:

RO

B.2.2.4.42 CLUSTERROM\_PIDR5, Cluster ROM table Peripheral Identification Register 5

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFD4

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-316: EXT\_CLUSTERROM\_PIDR5 bit assignments

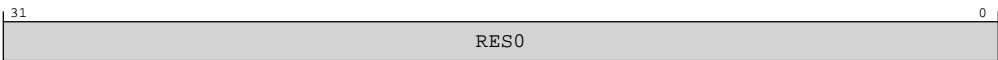


Table B-612: CLUSTERROM\_PIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFD4	None

This interface is accessible as follows:

RO

B.2.2.4.43 CLUSTERROM\_PIDR6, Cluster ROM table Peripheral Identification Register 6

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFD8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-317: EXT\_CLUSTERROM\_PIDR6 bit assignments

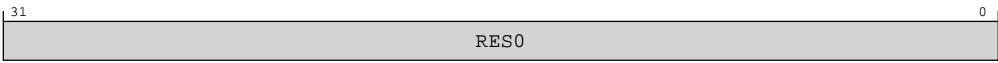


Table B-614: CLUSTERROM\_PIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFD8	None

This interface is accessible as follows:

RO

B.2.2.4.44 CLUSTERROM\_PIDR7, Cluster ROM table Peripheral Identification Register 7

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFDC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-318: EXT\_CLUSTERROM\_PIDR7 bit assignments

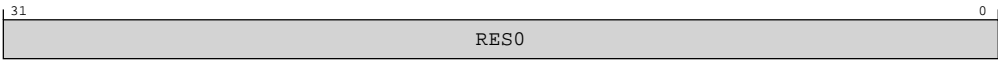


Table B-616: CLUSTERROM\_PIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
CLUSTERROM	0xFDC	None

This interface is accessible as follows:

RO

B.2.2.4.45 CLUSTERROM\_PIDR0, Cluster ROM table Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFE0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-319: EXT\_CLUSTERROM\_PIDR0 bit assignments

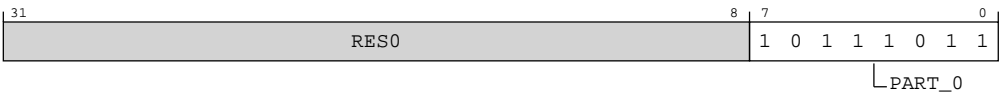


Table B-618: CLUSTERROM\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:0]	PART_0	Part number bits [7:0].  <b>0b10111011</b> Cortex-R82AE Cluster ROM table. Bits [7:0] of part number 0x4BB.	0xBB

Accessibility

Component	Offset	Range
CLUSTERROM	0xFE0	None

This interface is accessible as follows:

RO

B.2.2.4.46 CLUSTERROM\_PIDR1, Cluster ROM table Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFE4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-320: EXT\_CLUSTERROM\_PIDR1 bit assignments

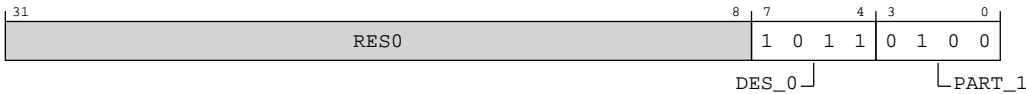


Table B-620: CLUSTERROM\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0]. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b0100</b> Cortex-R82AE Cluster ROM table. Bits [11:8] of part number 0x4BB.	0b0100

Accessibility

Component	Offset	Range
CLUSTERROM	0xFE4	None

This interface is accessible as follows:

RO

B.2.2.4.47 CLUSTERROM\_PIDR2, Cluster ROM table Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-321: EXT\_CLUSTERROM\_PIDR2 bit assignments

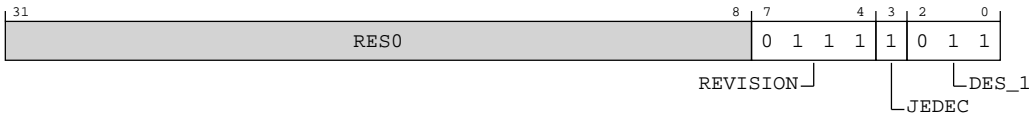


Table B-622: CLUSTERROM\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
CLUSTERROM	0xFE8	None

This interface is accessible as follows:

RO



B.2.2.4.48 CLUSTERROM\_PIDR3, Cluster ROM table Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFEC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-322: EXT\_CLUSTERROM\_PIDR3 bit assignments

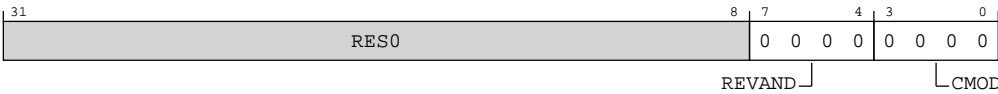


Table B-624: CLUSTERROM\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
CLUSTERROM	0xFEC	None

This interface is accessible as follows:

RO

B.2.2.4.49 CLUSTERROM\_CIDR0, Cluster ROM table Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFF0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	1101
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-323: EXT\_CLUSTERROM\_CIDR0 bit assignments

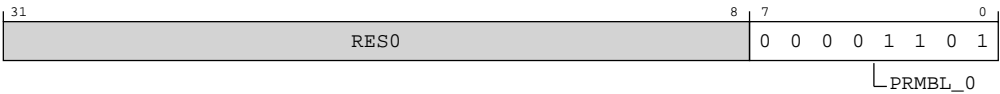


Table B-626: CLUSTERROM\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble.  <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
CLUSTERROM	0xFF0	None

This interface is accessible as follows:

RO

B.2.2.4.50 CLUSTERROM\_CIDR1, Cluster ROM table Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

Register offset

0xFF4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-324: EXT\_CLUSTERROM\_CIDR1 bit assignments

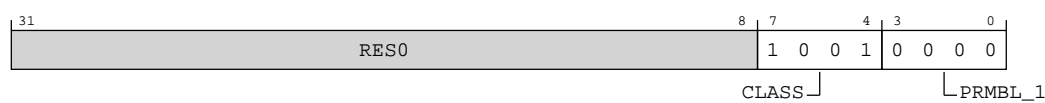


Table B-628: CLUSTERROM\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1001</b> CoreSight component.	0b1001
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
CLUSTERROM	0xFF4	None

This interface is accessible as follows:

RO

B.2.2.4.51 CLUSTERROM\_CIDR2, Cluster ROM table Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

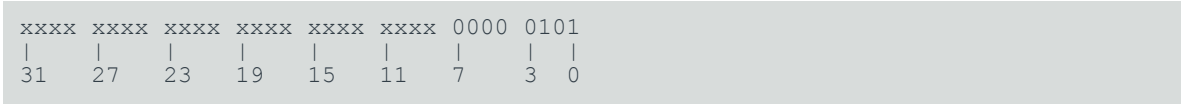
Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-325: EXT\_CLUSTERROM\_CIDR2 bit assignments



Table B-630: CLUSTERROM\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble. <b>0b000000101</b> CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
CLUSTERROM	0xFF8	None

This interface is accessible as follows:

RO

B.2.2.4.52 CLUSTERROM\_CIDR3, Cluster ROM table Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CLUSTERROM

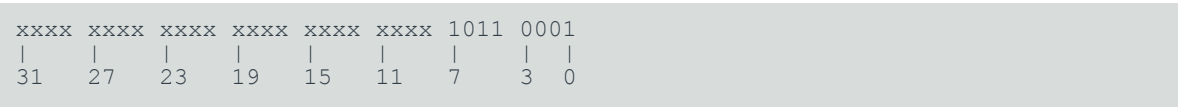
Register offset

0xFFC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-326: EXT\_CLUSTERROM\_CIDR3 bit assignments



Table B-632: CLUSTERROM\_CIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble. <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
CLUSTERROM	0xFFC	None

This interface is accessible as follows:

RO

B.2.2.5 External COREROM register description

This section includes the register descriptions for all memory-mapped COREROM registers that are accessed for each core.

B.2.2.5.1 COREROM\_ROMENTRY0, Core ROM table Entry 0

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0x000

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x011
31	27	23	19	15	11	7	3	0

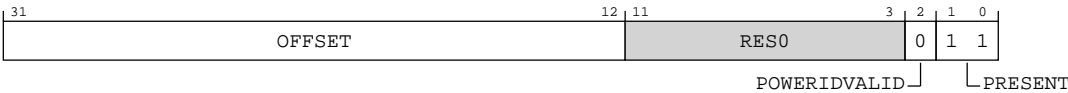


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-327: EXT\_COREROM\_ROMENTRY0 bit assignments



**Table B-634: COREROM\_ROMENTRY0 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000001</b></p> <p>Core Debug at ROM table address + 0x1000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000000000010000</b></p> <p>Core Debug at ROM table address + 0x1_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b></p> <p>The ROM Entry is present.</p>	0b11

### Accessibility

Component	Offset	Range
COREROM	0x000	None

This interface is accessible as follows:

RO

#### B.2.2.5.2 COREROM\_ROMENTRY1, Core ROM table Entry 1

Provides the address offset for one CoreSight component.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

COREROM



Register offset

0x004

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x011
31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-328: EXT\_COREROM\_ROMENTRY1 bit assignments

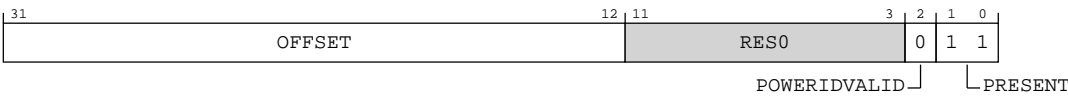


Table B-636: COREROM\_ROMENTRY1 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000010</b> Core PMU at ROM table address + 0x2000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>0000000000000000100000</b> Core PMU at ROM table address + 0x2_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	Indicates if the Power domain ID field contains a Power domain ID.  <b>0b0</b> A power domain ID is not provided.	0b0
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table.  <b>0b11</b> The ROM Entry is present.	0b11

Accessibility

Component	Offset	Range
COREROM	0x004	None

This interface is accessible as follows:

RO

B.2.2.5.3 COREROM\_ROMENTRY2, Core ROM table Entry 2

Provides the address offset for one CoreSight component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0x008

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x011
31	27	23	19	15	11	7	3	0

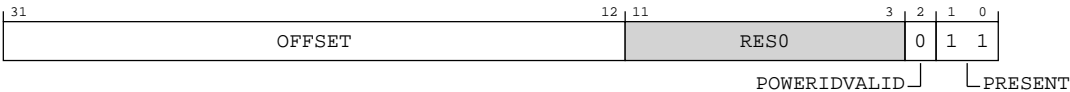


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-329: EXT\_COREROM\_ROMENTRY2 bit assignments



**Table B-638: COREROM\_ROMENTRY2 bit descriptions**

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000011</b></p> <p>Core Trace at ROM table address + 0x3000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000110000</b></p> <p>Core Trace at ROM table address + 0x3_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0
[1:0]	PRESENT	<p>Indicates whether an entry is present at this location in the ROM Table.</p> <p><b>0b11</b></p> <p>The ROM Entry is present.</p>	0b11

### Accessibility

Component	Offset	Range
COREROM	0x008	None

This interface is accessible as follows:

RO

#### B.2.2.5.4 COREROM\_ROMENTRY3, Core ROM table Entry 3

Provides the address offset for one CoreSight component.

### Configurations

This register is available in all configurations.

### Attributes

#### Width

32

#### Component

COREROM

Register offset

0x00C

Access type

RO

Reset value

When ELA == 1

XXXX XXXX XXXX XXXX XXXX XXXX XXXX x011

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX



Where the reset reads xxxx, see individual bits.

Bit descriptions

When ELA == 1

Figure B-330: EXT\_COREROM\_ROMENTRY3 bit assignments

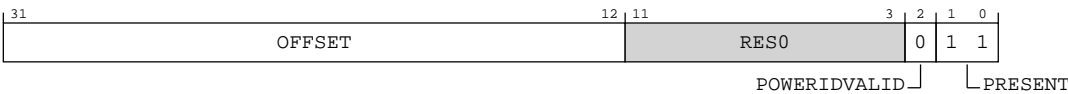


Table B-640: COREROM\_ROMENTRY3 bit descriptions

Bits	Name	Description	Reset
[31:12]	OFFSET	<p><b>When DENSE_CS_ADDR_MAP == 1</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>00000000000000000000100</b> Core ELA at ROM table address + 0x4000.</p> <p><b>Otherwise</b></p> <p>The component address, relative to the base address of this ROM Table. The component address is calculated using the following equation: Component Address = ROM Table Base Address + (OFFSET &lt;&lt; 12).</p> <p><b>000000000000000001000000</b> Core ELA at ROM table address + 0x4_0000.</p>	20 {x}
[11:3]	RES0	Reserved	RES0
[2]	POWERIDVALID	<p>Indicates if the Power domain ID field contains a Power domain ID.</p> <p><b>0b0</b></p> <p>A power domain ID is not provided.</p>	0b0

Bits	Name	Description	Reset
[1:0]	PRESENT	Indicates whether an entry is present at this location in the ROM Table.  <b>0b11</b> The ROM Entry is present.	0b11

Figure B-331: EXT\_COREROM\_ROMENTRY3 bit assignments

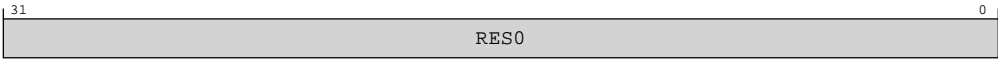


Table B-641: COREROM\_ROMENTRY3 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0x00C	None

This interface is accessible as follows:

RO

B.2.2.5.5 COREROM\_PRIDR0, Core ROM table Power Request ID Register 0

Indicates the features of the power request functionality.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xC00

Access type

RO

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-332: EXT\_COREROM\_PRIDR0 bit assignments

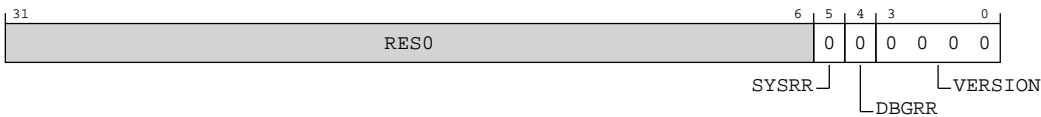


Table B-643: COREROM\_PRIDR0 bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	SYSRR	System reset request functionality present. <b>0b0</b> The system reset request functionality is not implemented.	0b0
[4]	DBGRR	Debug reset request functionality present. <b>0b0</b> The debug reset request functionality is not implemented.	0b0
[3:0]	VERSION	Version of the power request functionality. <b>0b0000</b> The power request functionality is not implemented.	0b0000

Accessibility

Component	Offset	Range
COREROM	0xC00	None

This interface is accessible as follows:

RO

B.2.2.5.6 COREROM\_ITCTRL, Core ROM table Integration Mode Control Register

No functional/integration mode switching implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width  
32

Component  
COREROM

Register offset  
0xF00

Access type  
RW

Reset value

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxx0

31

27

23

19

15

11

7

3

0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-333: EXT\_COREROM\_ITCTRL bit assignments

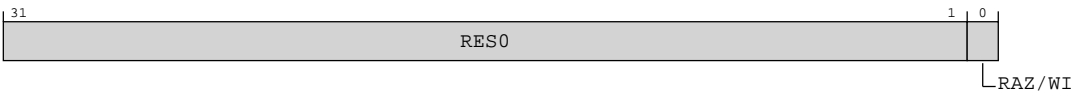


Table B-645: COREROM\_ITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
COREROM	0xF00	None

This interface is accessible as follows:

RW

B.2.2.5.7     COREROM\_CLAIMSET, Core ROM table Claim Tag Set Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFA0

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-334: EXT\_COREROM\_CLAIMSET bit assignments

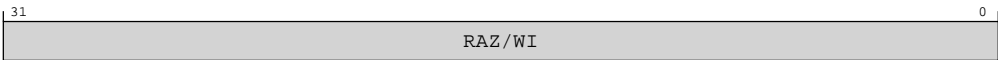


Table B-647: COREROM\_CLAIMSET bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
COREROM	0xFA0	None

This interface is accessible as follows:

RW



B.2.2.5.8     COREROM\_CLAIMCLR, Core ROM table Claim Tag Clear Register

No claim tags implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFA4

Access type

RW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-335: EXT\_COREROM\_CLAIMCLR bit assignments

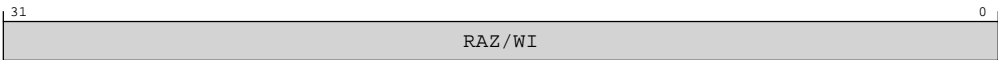


Table B-649: COREROM\_CLAIMCLR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
COREROM	0xFA4	None

This interface is accessible as follows:

RW

B.2.2.5.9     COREROM\_DEVAFF0, Core ROM table Device Affinity Register 0

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFA8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-336: EXT\_COREROM\_DEVAFF0 bit assignments

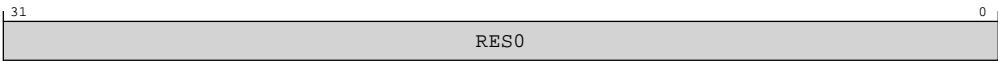


Table B-651: COREROM\_DEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFA8	None

This interface is accessible as follows:

RO

B.2.2.5.10 COREROM\_DEVAFF1, Core ROM table Device Affinity Register 1

Enables a debugger to determine whether two components have an affinity with each other.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFAC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-337: EXT\_COREROM\_DEVAFF1 bit assignments

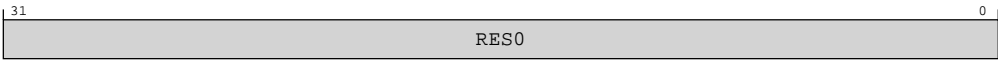


Table B-653: COREROM\_DEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFAC	None

This interface is accessible as follows:

RO

B.2.2.5.11 COREROM\_LAR, Core ROM table Software Lock Access Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFB0

Access type

RESERVEDW

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-338: EXT\_COREROM\_LAR bit assignments



Table B-655: COREROM\_LAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
COREROM	0xFB0	None

This interface is accessible as follows:

WO

B.2.2.5.12 COREROM\_LSR, Core ROM table Software Lock Status Register

No software locking implemented for ROM tables.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFB4

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-339: EXT\_COREROM\_LSR bit assignments

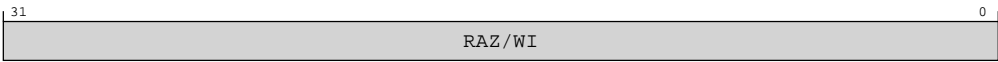


Table B-657: COREROM\_LSR bit descriptions

Bits	Name	Description	Reset
[31:0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Range
COREROM	0xFB4	None

This interface is accessible as follows:

RO

B.2.2.5.13 COREROM\_AUTHSTATUS, Core ROM table Authentication Status Register

Provides information about the state of the authentication interface for debug.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFB8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-340: EXT\_COREROM\_AUTHSTATUS bit assignments

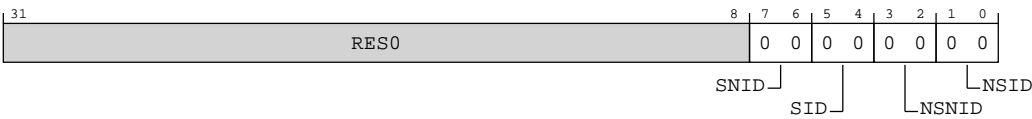


Table B-659: COREROM\_AUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Secure Non-invasive Debug.  0b00  Debug level is not supported.	0b00

Bits	Name	Description	Reset
[5:4]	SID	Secure Invasive Debug. <b>0b00</b> Debug level is not supported.	0b00
[3:2]	NSNID	Non-secure Non-invasive Debug. <b>0b00</b> Debug level is not supported.	0b00
[1:0]	NSID	Non-secure Invasive Debug. <b>0b00</b> Debug level is not supported.	0b00

## Accessibility

Component	Offset	Range
COREROM	0xFB8	None

This interface is accessible as follows:

RO

### B.2.2.5.14 COREROM\_DEVARCH, Core ROM table Device Architecture Register

Identifies the architect and architecture of a CoreSight component.

## Configurations

This register is available in all configurations.

## Attributes

### Width

32

### Component

COREROM

### Register offset

0xFBC

### Access type

RO

### Reset value

0100 0111 0111 0000 0000 1010 1111 0111

Bit descriptions

Figure B-341: EXT\_COREROM\_DEVARCH bit assignments

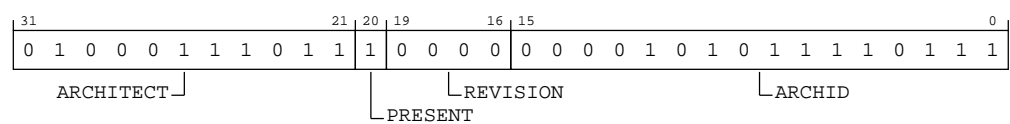


Table B-661: COREROM\_DEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect.  0b01000111011 JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	Present.  0b1 DEVARCH information present.	0b1
[19:16]	REVISION	Revision.  0b0000 Revision 0.	0b0000
[15:0]	ARCHID	Architecture ID.  0b000010101110111 ROM Table v0. The debug tool must inspect ext-COREROM_DEVTYPE and ext-COREROM_DEVID to determine further information about the ROM Table.	0x0AF7

Accessibility

Component	Offset	Range
COREROM	0xFBC	None

This interface is accessible as follows:

RO

B.2.2.5.15 COREROM\_DEVID2, Core ROM table Device Configuration Register 2

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32



**Component**  
COREROM

**Register offset**  
0xFC0

**Access type**  
RO

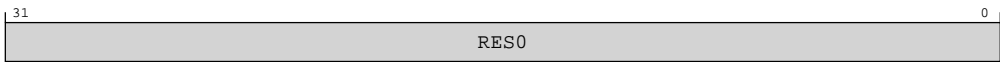
**Reset value**



Where the reset reads xxxx, see individual bits.

**Bit descriptions**

**Figure B-342: EXT\_COREROM\_DEVID2 bit assignments**



**Table B-663: COREROM\_DEVID2 bit descriptions**

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

**Accessibility**

Component	Offset	Range
COREROM	0xFC0	None

This interface is accessible as follows:

RO

**B.2.2.5.16 COREROM\_DEVID1, Core ROM table Device Configuration Register 1**

Indicates the capabilities of the component.

**Configurations**

This register is available in all configurations.

Attributes

Width  
32

Component  
COREROM

Register offset  
0xFC4

Access type  
RO

Reset value

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

31

27

23

19

15

11

7

3

0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-343: EXT\_COREROM\_DEVID1 bit assignments

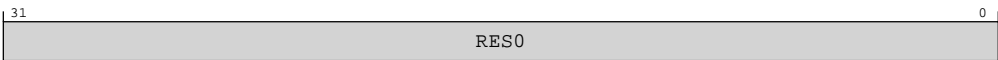


Table B-665: COREROM\_DEVID1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFC4	None

This interface is accessible as follows:

RO

B.2.2.5.17 COREROM\_DEVID, Core ROM table Device Configuration Register

Indicates the capabilities of the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFC8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-344: EXT\_COREROM\_DEVID bit assignments

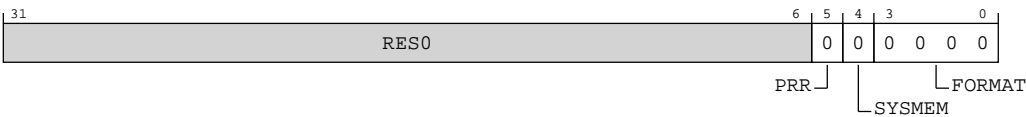


Table B-667: COREROM\_DEVID bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	PRR	Power Request functionality included.  0b0 Power Request functionality not included.	0b0

Bits	Name	Description	Reset
[4]	SYMEM	System memory present.  <b>0b0</b> System memory is not present on the bus.	0b0
[3:0]	FORMAT	ROM format.  <b>0b0000</b> 32-bit format 0.	0b0000

Accessibility

Component	Offset	Range
COREROM	0xFC8	None

This interface is accessible as follows:

RO

B.2.2.5.18 COREROM\_DEVTYPE, Core ROM table Device Type Register

A debugger can use DEVTYPE to obtain information about a component that has an unrecognized part number.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFCC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-345: EXT\_COREROM\_DEVTYPE bit assignments



Table B-669: COREROM\_DEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Sub number <b>0b0000</b> Other, undefined.	0b0000
[3:0]	MAJOR	Major number <b>0b0000</b> Miscellaneous.	0b0000

Accessibility

Component	Offset	Range
COREROM	0xFCC	None

This interface is accessible as follows:

RO

B.2.2.5.19 COREROM\_PIDR4, Core ROM table Peripheral Identification Register 4

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

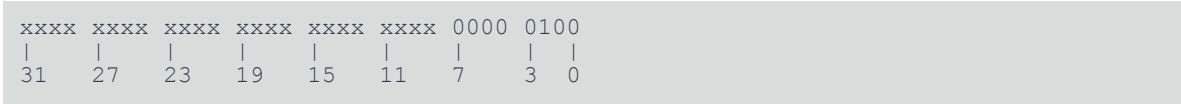
Register offset

0xFD0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-346: EXT\_COREROM\_PIDR4 bit assignments



Table B-671: COREROM\_PIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count. <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code. <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
COREROM	0xFD0	None

This interface is accessible as follows:

RO

B.2.2.5.20 COREROM\_PIDR5, Core ROM table Peripheral Identification Register 5

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width  
32

Component  
COREROM

Register offset  
0xFD4

Access type  
RO

Reset value

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

xxxx

31

27

23

19

15

11

7

3

0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-347: EXT\_COREROM\_PIDR5 bit assignments

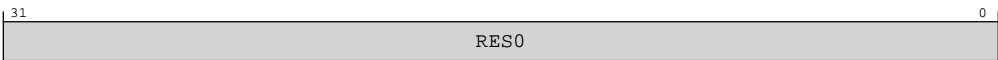


Table B-673: COREROM\_PIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFD4	None

This interface is accessible as follows:

RO

B.2.2.5.21 COREROM\_PIDR6, Core ROM table Peripheral Identification Register 6

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFD8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-348: EXT\_COREROM\_PIDR6 bit assignments

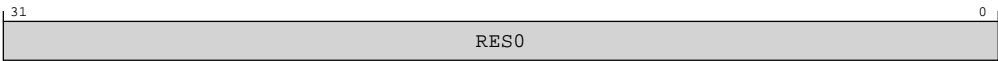


Table B-675: COREROM\_PIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFD8	None

This interface is accessible as follows:



RO

B.2.2.5.22 COREROM\_PIDR7, Core ROM table Peripheral Identification Register 7

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFDC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-349: EXT\_COREROM\_PIDR7 bit assignments

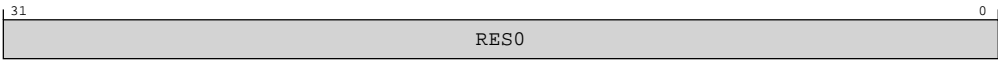


Table B-677: COREROM\_PIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
COREROM	0xFDC	None

This interface is accessible as follows:

RO

B.2.2.5.23 COREROM\_PIDR0, Core ROM table Peripheral Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFE0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-350: EXT\_COREROM\_PIDR0 bit assignments

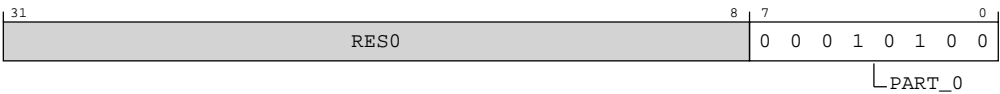


Table B-679: COREROM\_PIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:0]	PART_0	Part number bits [7:0].  <b>0b00010100</b> Cortex-R82AE Core ROM table. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Range
COREROM	0xFE0	None

This interface is accessible as follows:

RO

B.2.2.5.24 COREROM\_PIDR1, Core ROM table Peripheral Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFE4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	1101
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-351: EXT\_COREROM\_PIDR1 bit assignments



Table B-681: COREROM\_PIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0]. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b1101</b> Cortex-R82AE Core ROM table. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Range
COREROM	0xFE4	None

This interface is accessible as follows:

RO

B.2.2.5.25 COREROM\_PIDR2, Core ROM table Peripheral Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

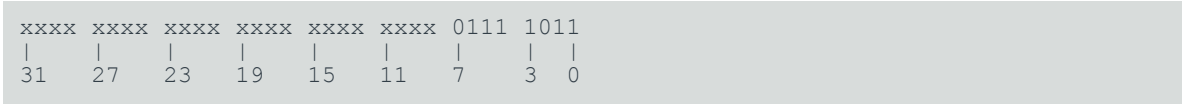
Register offset

0xFE8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-352: EXT\_COREROM\_PIDR2 bit assignments

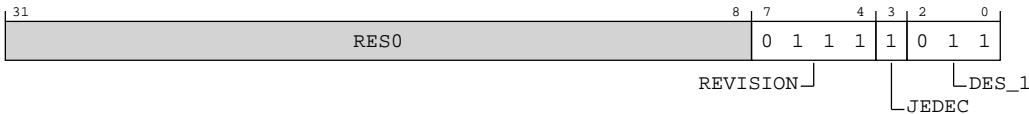


Table B-683: COREROM\_PIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
COREROM	0xFE8	None

This interface is accessible as follows:

RO

B.2.2.5.26 COREROM\_PIDR3, Core ROM table Peripheral Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFEC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-353: EXT\_COREROM\_PIDR3 bit assignments

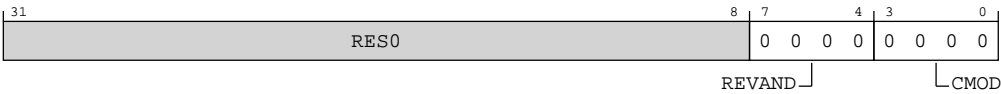


Table B-685: COREROM\_PIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
COREROM	0xFEC	None

This interface is accessible as follows:

RO

B.2.2.5.27 COREROM\_CIDR0, Core ROM table Component Identification Register 0

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFF0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	1101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-354: EXT\_COREROM\_CIDR0 bit assignments



Table B-687: COREROM\_CIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	CoreSight component identification preamble.  0b00001101 CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
COREROM	0xFF0	None

This interface is accessible as follows:

RO

B.2.2.5.28 COREROM\_CIDR1, Core ROM table Component Identification Register 1

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFF4

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure B-355: EXT\_COREROM\_CIDR1 bit assignments

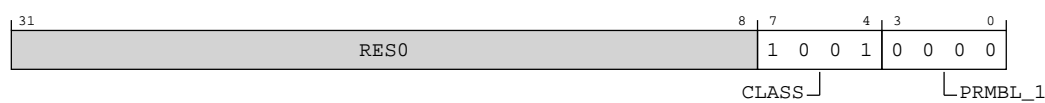


Table B-689: COREROM\_CIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	CoreSight component class. <b>0b1001</b> CoreSight component.	0b1001
[3:0]	PRMBL_1	CoreSight component identification preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
COREROM	0xFF4	None

This interface is accessible as follows:

RO

B.2.2.5.29 COREROM\_CIDR2, Core ROM table Component Identification Register 2

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

COREROM

Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-356: EXT\_COREROM\_CIDR2 bit assignments



Table B-691: COREROM\_CIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	CoreSight component identification preamble. <b>0b000000101</b> CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
COREROM	0xFF8	None

This interface is accessible as follows:

RO

B.2.2.5.30 COREROM\_CIDR3, Core ROM table Component Identification Register 3

Provides CoreSight discovery information.

Configurations

This register is available in all configurations.

Attributes

Width

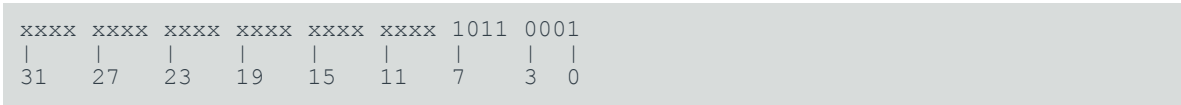
32

Component  
COREROM

Register offset  
0xFFC

Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-357: EXT\_COREROM\_CIDR3 bit assignments



Table B-693: COREROM\_CIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	CoreSight component identification preamble.  0b10110001 CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
COREROM	0xFFC	None

This interface is accessible as follows:

RO

B.2.2.6 External CTI register description

This section includes the register descriptions for all memory-mapped *Cross Trigger Interface* (CTI) registers that are accessed for both the cluster and each core.

B.2.2.6.1 CTICONTROL, CTI Control register

Controls whether the CTI is enabled.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

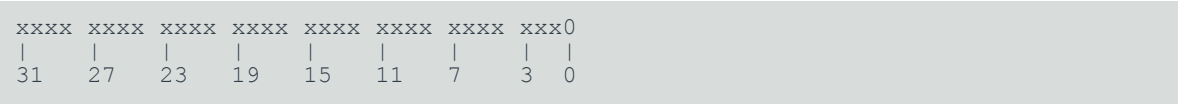
Register offset

0x000

Access type

RW

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-358: EXT\_CTICONTROL bit assignments

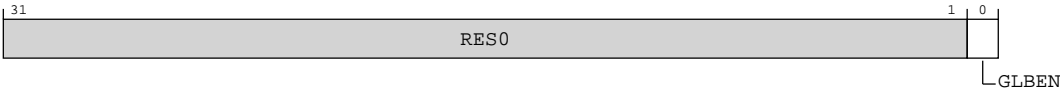


Table B-695: CTICONTROL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	GLBEN	<div>Enables or disables the CTI mapping functions. Possible values of this field are:</div> <div><div><div>0b0</div><div>CTI mapping functions and application trigger disabled.</div></div><div><div>0b1</div><div>CTI mapping functions and application trigger enabled.</div></div></div> <div>When GLBEN is 0, the input channel to output trigger, input trigger to output channel, and application trigger functions are disabled and do not signal new events on either output triggers or output channels. If a previously asserted output trigger has not been acknowledged, it is <b>CONSTRAINED UNPREDICTABLE</b>, and the implemented behavior is:</div> <div><div><div><div></div><div>The output trigger remains asserted after the mapping functions are disabled.</div></div></div></div> <div>All output triggers are disabled by CTI reset.</div> <div>If the ECT supports multicycle channel events any existing output channel events will be terminated.</div>	0b0

Accessibility

Component	Offset	Instance	Range
CTI	0x000	CTICONTROL	None

This interface is accessible as follows:

RW

B.2.2.6.2 CTIINTACK, CTI Output Trigger Acknowledge register

Can be used to deactivate the output triggers.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x010

Access type

Read

RESERVED

Write

W

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-359: EXT\_CTIINTACK bit assignments**

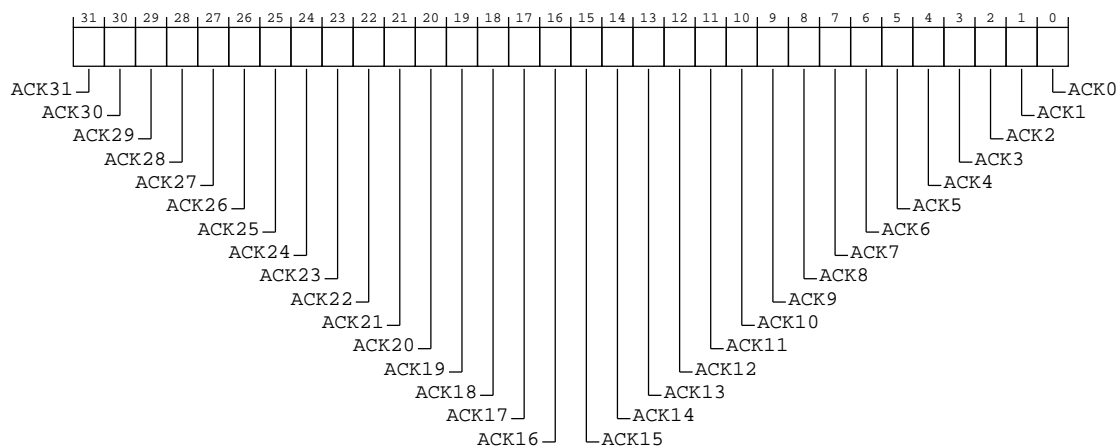


Table B-697: CTIINTACK bit descriptions

Bits	Name	Description	Reset
[31:0]	ACK<n>, bit[n], where n = 31 to 0	<p>Acknowledge for output trigger &lt;n&gt;.</p> <p>Bits [31:N] are <b>RAZ/WI</b>. N is the number of CTI triggers implemented as defined by the ext-CTIDEVID.NUMTRIG field.</p> <p>If any of the following is true, writes to ACK&lt;n&gt; are ignored:</p> <ul style="list-style-type: none"><li>n &gt;= ext-CTIDEVID.NUMTRIG, the number of implemented triggers.</li><li>Output trigger n is not active.</li><li>The channel mapping function output, as controlled by ext-CTIOUTEN&lt;n&gt;, is still active.</li><li>Output trigger n is not implemented.</li><li>Output trigger n is not connected.</li><li>Output trigger n is self-acknowledging and does not require software acknowledge.</li></ul> <p>Otherwise, the behavior on writes to ACK&lt;n&gt; is as follows:</p> <p><b>0b0</b></p> <p>No effect</p> <p><b>0b1</b></p> <p>Deactivate the trigger.</p>	32 {x}

Accessibility

A debugger must read ext-CTITRIGOUTSTATUS to confirm that the output trigger has been acknowledged before generating any event that must be ordered after the write to CTIINTACK, such as a write to CTIAPPPULSE to activate another trigger.

Component	Offset	Instance	Range
CTI	0x010	CTIINTACK	None

This interface is accessible as follows:

WO

B.2.2.6.3 CTIAPPSET, CTI Application Trigger Set register

Sets the application triggers.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x014

Access type

RW1S

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-360: EXT\_CTIAPPSET bit assignments

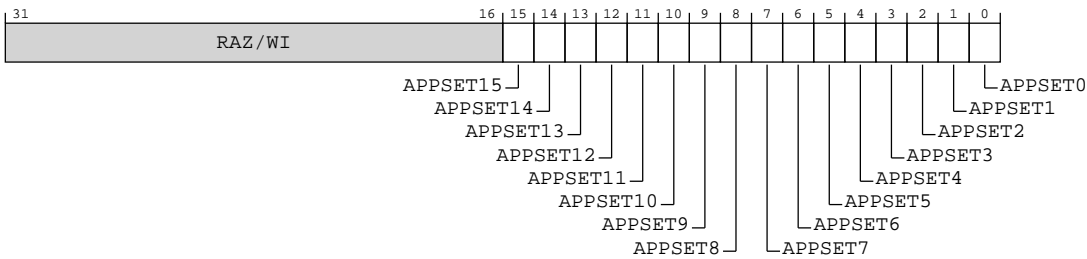


Table B-699: CTIAPPSET bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI
[15:0]	APPSET<x>, bit[x], where x = 15 to 0	<p>Application trigger &lt;x&gt; enable.</p> <p>Bits [31:N] are <b>RAZ/WI</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</p> <p><b>0b0</b></p> <p>Reading this means the application trigger is inactive. Writing this has no effect.</p> <p><b>0b1</b></p> <p>Reading this means the application trigger is active. Writing this sets the corresponding application trigger to 1 and generates a channel event.</p> <p>If the ECT does not support multicycle channel events, use of CTIAPPSET is deprecated and the debugger must only use ext-CTIAPPULSE.</p>	16{x}



Accessibility

Component	Offset	Instance	Range
CTI	0x014	CTIAPPSET	None

This interface is accessible as follows:

RW

B.2.2.6.4 CTIAPPCLEAR, CTI Application Trigger Clear register

Clears the application triggers.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x018

Access type

RESERVEDW

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-361: EXT\_CTIAPPCLEAR bit assignments

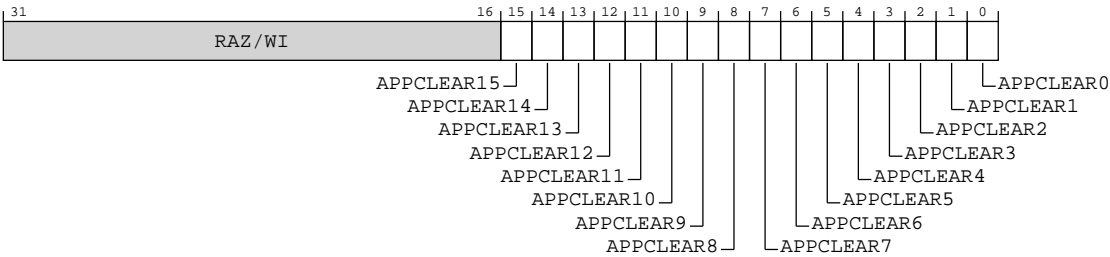


Table B-701: CTIAPPCLEAR bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI
[15:0]	APPCLEAR<x>, bit[x], where x = 15 to 0	<p>Application trigger &lt;x&gt; disable.</p> <p>Bits [31:N] are <b>RAZ/WI</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</p> <p>Writing to this bit has the following effect:</p> <p><b>0b0</b></p> <p>No effect.</p> <p><b>0b1</b></p> <p>Clear corresponding application trigger to 0 and clear the corresponding channel event.</p> <p>If the ECT does not support multicycle channel events, use of CTIAPPCLEAR is deprecated and the debugger must only use ext-CTIAPPPULSE.</p>	16{x}

Accessibility

Component	Offset	Instance	Range
CTI	0x018	CTIAPPCLEAR	None

This interface is accessible as follows:

WO

B.2.2.6.5 CTIAPPPULSE, CTI Application Pulse register

Causes event pulses to be generated on ECT channels.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x01C

Access type

Read

RESERVED

Write

W

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx	
31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-362: EXT\_CTIAPPPULSE bit assignments

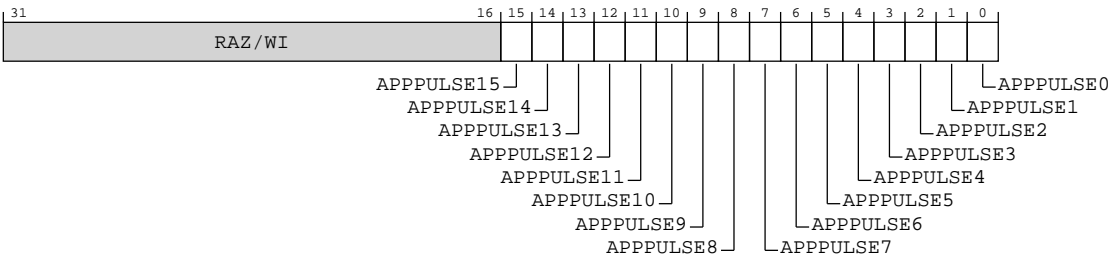


Table B-703: CTIAPPPULSE bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI

Bits	Name	Description	Reset
[15:0]	APPPULSE<x>, bit[x], where x = 15 to 0	<p>Generate event pulse on ECT channel &lt;x&gt;.</p> <p>Bits [31:N] are <b>RAZ/WI</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</p> <p>Writing to this bit has the following effect:</p> <p><b>0b0</b></p> <p>No effect.</p> <p><b>0b1</b></p> <p>Channel &lt;x&gt; event pulse generated.</p> <ul style="list-style-type: none"> <li>The CTIAPPPULSE operation does not affect the state of the application trigger. If the channel is active, either because of an earlier event or from the application trigger, then the value written to CTIAPPPULSE might have no effect.</li> <li>Multiple pulse events that occur close together might be merged into a single pulse event.</li> </ul>	16 {x}

### Accessibility

It is CONSTRAINED UNPREDICTABLE whether a write to CTIAPPPULSE generates an event on a channel if CTICONTROL.GLBEN is 0.

Component	Offset	Instance	Range
CTI	0x01C	CTIAPPPULSE	None

This interface is accessible as follows:

WO

#### B.2.2.6.6 CTIINEN<n>, CTI Input Trigger to Output Channel Enable registers, n = 0 - 9

Enables the signaling of an event on output channels when input trigger event n is received by the CTI.

### Configurations

If input trigger n is not connected, the programming of CTIINEN<n> is ignored.

### Attributes

#### Width

32

#### Component

CTI

#### Register offset

0x020 + (4 \* n)

#### Access type

RW

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-363: EXT\_CTIINEN<n> bit assignments

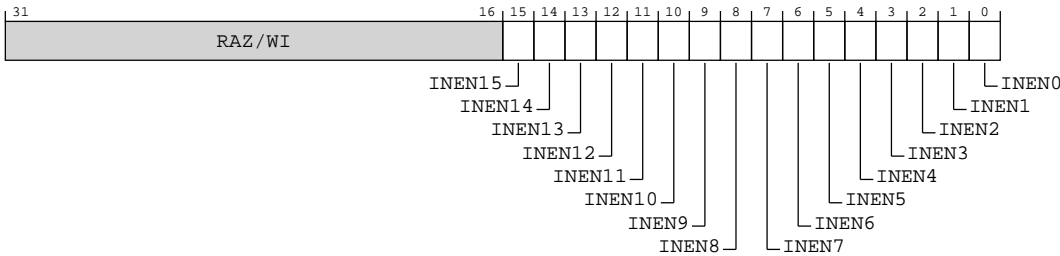


Table B-705: CTIINEN<n> bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI
[15:0]	INEN<x>, bit[x], where x = 15 to 0	Input trigger <n> to output channel <x> enable.  Bits [31:N] are <b>RAZ/WI</b> . N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.  <b>0b0</b> Input trigger <n> will not generate an event on output channel <x>.  <b>0b1</b> Input trigger <n> will generate an event on output channel <x>.	16 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0x020 + (4 * n)	CTIINEN<n>	None

This interface is accessible as follows:

RW

B.2.2.6.7 CTIOUTEN<n>, CTI Input Channel to Output Trigger Enable registers, n = 0 - 9

Defines which input channels generate output trigger n.

Configurations

If output trigger n is not connected, the programming of CTIOUTEN<n> is ignored.

Attributes

Width

32

Component

CTI

Register offset

0x0A0 + (4 \* n)

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-364: EXT\_CTIOUTEN<n> bit assignments

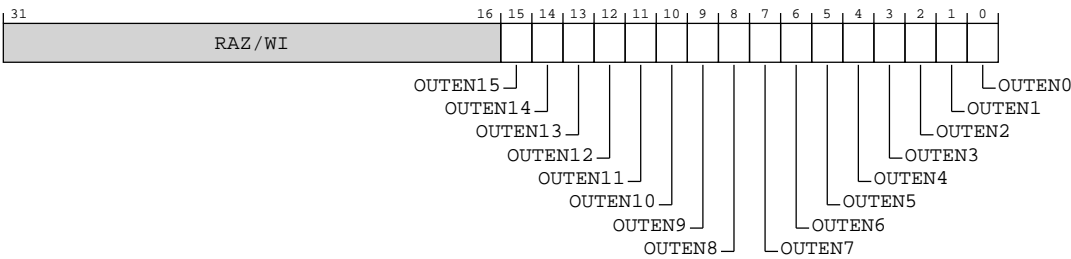


Table B-707: CTIOUTEN<n> bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI

Bits	Name	Description	Reset
[15:0]	OUTEN<x>, bit[x], where x = 15 to 0	<div>Input channel &lt;x&gt; to output trigger &lt;n&gt; enable.</div> <div>Bits [31:N] are <b>RAZ/WI</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</div> <div>Possible values of this bit are:</div> <div><b>0b0</b><div>An event on input channel &lt;x&gt; will not cause output trigger &lt;n&gt; to be asserted.</div></div> <div><b>0b1</b><div>An event on input channel &lt;x&gt; will cause output trigger &lt;n&gt; to be asserted.</div></div>	16 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0x0A0 + (4 * n)	CTIOUTEN<n>	None

This interface is accessible as follows:

RW

B.2.2.6.8 CTITRIGINSTATUS, CTI Trigger In Status register

Provides the status of the trigger inputs.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x130

Access type

RO

Reset value

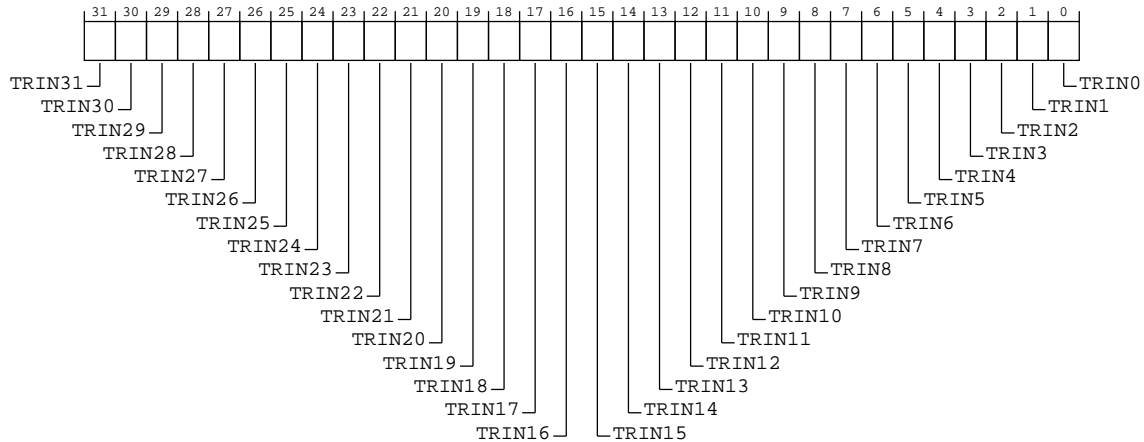
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-365: EXT\_CTITRIGINSTATUS bit assignments**



**Table B-709: CTITRIGINSTATUS bit descriptions**

Bits	Name	Description	Reset
[31:0]	TRIN<n>, bit[n], where n = 31 to 0	<p>Trigger input &lt;n&gt; status.</p> <p>Bits [31:N] are <b>RAZ</b>. N is the number of CTI triggers implemented as defined by the ext-CTIDEVID.NUMTRIG field.</p> <p><b>0b0</b></p> <p>Input trigger n is inactive.</p> <p><b>0b1</b></p> <p>Input trigger n is active.</p> <p>Not implemented and not-connected input triggers are always inactive.</p> <p>It is IMPLEMENTATION DEFINED whether an input trigger that does not support multicyle events can be observed as active.</p> <p>Input triggers that do not support multicyle events might be observed as active.</p>	32 {x}

## Accessibility

Component	Offset	Instance	Range
CTI	0x130	CTITRIGINSTATUS	None

This interface is accessible as follows:



RO

B.2.2.6.9 CTITRIGOUTSTATUS, CTI Trigger Out Status register

Provides the raw status of the trigger outputs, after processing by any **IMPLEMENTATION DEFINED** trigger interface logic. For output triggers that are self-acknowledging, this is only meaningful if the CTI implements multicycle channel events.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x134

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-366: EXT\_CTITRIGOUTSTATUS bit assignments

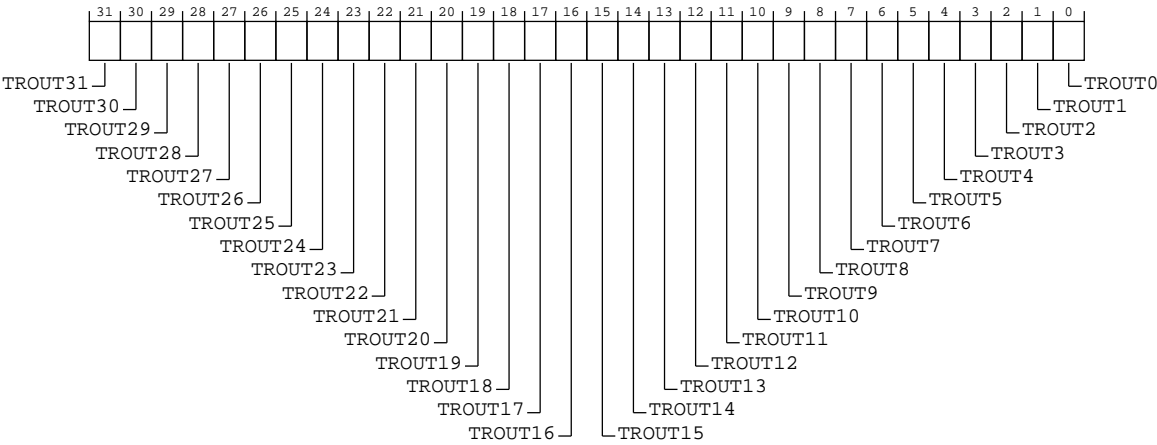


Table B-711: CTITRIGOUTSTATUS bit descriptions

Bits	Name	Description	Reset
[31:0]	TROUT<n>, bit[n], where n = 31 to 0	<p>Trigger output &lt;n&gt; status.</p> <p>Bits [31:N] are <b>RAZ</b>. N is the value in ext-CTIDEVID.NUMTRIG.</p> <p>If n &lt; N, and output trigger &lt;n&gt; is implemented and connected, and either the trigger is not self-acknowledging or the CTI implements multicycle channel events, then permitted values for TROUT&lt;n&gt; are:</p> <p><b>0b0</b></p> <p>Output trigger n is inactive.</p> <p><b>0b1</b></p> <p>Output trigger n is active.</p> <p>Otherwise when n &lt; N TROUT&gt;n&lt; is <b>RAZ</b>.</p>	32 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0x134	CTITRIGOUTSTATUS	None

This interface is accessible as follows:

RO

B.2.2.6.10 CTICHINSTATUS, CTI Channel In Status register

Provides the raw status of the ECT channel inputs to the CTI.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x138

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-367: EXT\_CTICHINSTATUS bit assignments

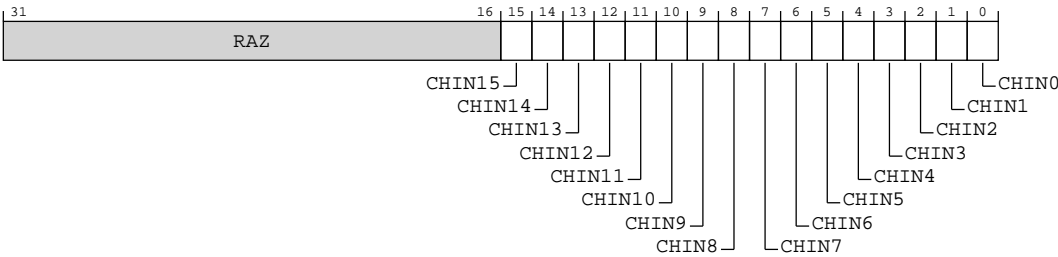


Table B-713: CTICHINSTATUS bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ	Reserved	RAZ

Bits	Name	Description	Reset
[15:0]	CHIN<n>, bit[n], where n = 15 to 0	<div>Input channel &lt;n&gt; status.</div> <div>Bits [31:N] are <b>RAZ</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</div> <div><b>0b0</b> Input channel &lt;n&gt; is inactive.</div> <div><b>0b1</b> Input channel &lt;n&gt; is active.</div>	16 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0x138	CTICHINSTATUS	None

This interface is accessible as follows:

RO

B.2.2.6.11 CTICHOUTSTATUS, CTI Channel Out Status register

Provides the status of the ECT channel outputs from the CTI.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x13C

Access type

RO

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-368: EXT\_CTICHOUTSTATUS bit assignments

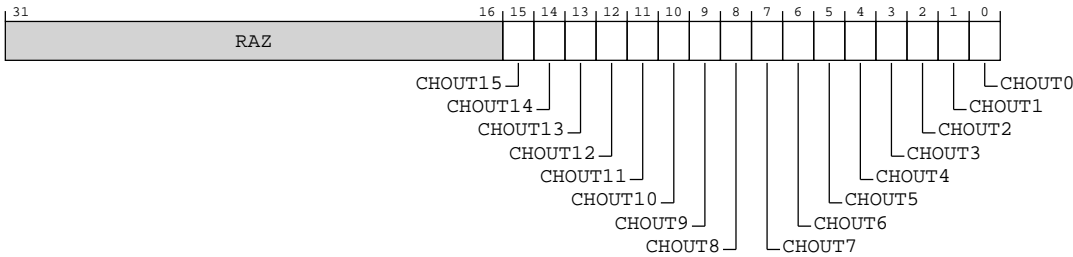


Table B-715: CTICHOUTSTATUS bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ	Reserved	RAZ
[15:0]	CHOUT<n>, bit[n], where n = 15 to 0	<p>Output channel &lt;n&gt; status.</p> <p>Bits [31:N] are <b>RAZ</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</p> <p>Possible values of this bit are:</p> <p><b>0b0</b></p> <p>Output channel &lt;n&gt; is inactive.</p> <p><b>0b1</b></p> <p>Output channel &lt;n&gt; is active.</p> <p><b>Note:</b></p> <p>The value in CTICHOUTSTATUS is after gating by the channel gate. For more information, see ext-CTIGATE.</p>	16{x}

Accessibility

Component	Offset	Instance	Range
CTI	0x13C	CTICHOUTSTATUS	None

This interface is accessible as follows:

RO

B.2.2.6.12 CTIGATE, CTI Channel Gate Enable register

Determines whether events on channels propagate through the CTM to other ECT components, or from the CTM into the CTI.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0x140

Access type

RW

Reset value

0000	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-369: EXT\_CTIGATE bit assignments

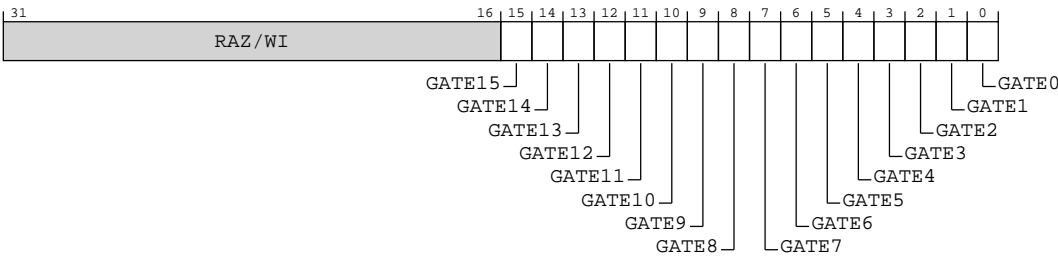


Table B-717: CTIGATE bit descriptions

Bits	Name	Description	Reset
[31:16]	RAZ/WI	Reserved	RAZ/WI

Bits	Name	Description	Reset
[15:0]	GATE<x>, bit[x], where x = 15 to 0	<p>Channel &lt;x&gt; gate enable.</p> <p>Bits [31:N] are <b>RAZ/WI</b>. N is the number of ECT channels implemented as defined by the ext-CTIDEVID.NUMCHAN field.</p> <p><b>0b0</b> Disable output and, if ext-CTIDEVID.INOUT == 0b01, input channel &lt;x&gt; propagation.</p> <p><b>0b1</b> Enable output and, if ext-CTIDEVID.INOUT == 0b01, input channel &lt;x&gt; propagation.</p> <p>If GATE&lt;x&gt; is set to 0, no new events will be propagated to the ECT, and if the ECT supports multicycle channel events any existing output channel events will be terminated.</p>	16 {x}

### Accessibility

Component	Offset	Instance	Range
CTI	0x140	CTIGATE	None

This interface is accessible as follows:

RW

#### B.2.2.6.13 ASICCTL, CTI External Multiplexer Control register

Can be used to provide **IMPLEMENTATION DEFINED** controls for the CTI. For example, the register might be used to control multiplexors for additional **IMPLEMENTATION DEFINED** triggers. The **IMPLEMENTATION DEFINED** controls provided by this register might modify the architecturally defined behavior of the CTI.



The architecturally-defined triggers must not be multiplexed.

### Configurations

In this implementation, this register is in the Debug power domain

#### Attributes

##### Width

32

##### Component

CTI

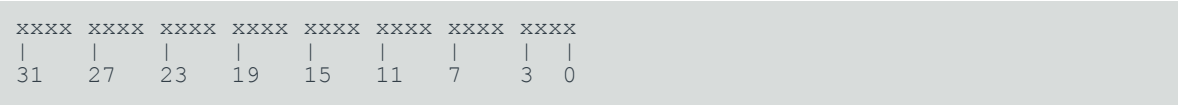
##### Register offset

0x144

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-370: EXT\_ASICCTL bit assignments



Table B-719: ASICCTL bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
CTI	0x144	ASICCTL	None

This interface is accessible as follows:

ImplementationDefined

B.2.2.6.14 CTIDEVCTL, CTI Device Control register

Provides target-specific device controls

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI



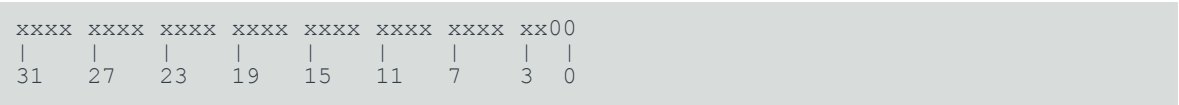
Register offset

0x150

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-371: EXT\_CTIDEVCTL bit assignments

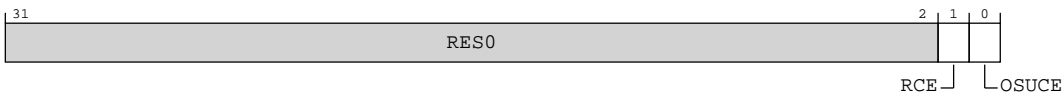


Table B-721: CTIDEVCTL bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	RCE	Reset Catch Enable.  0b0 Reset Catch debug event disabled.  0b1 Reset Catch debug event enabled.	0b0
[0]	OSUCE	OS Unlock Catch Enable  0b0 OS Unlock Catch debug event disabled.  0b1 OS Unlock Catch debug event enabled.	0b0

Accessibility

Component	Offset	Instance	Range
CTI	0x150	CTIDEVCTL	None

This interface is accessible as follows:

RW

B.2.2.6.15 CTIITCTRL, CTI Integration mode Control register

Enables the CTI to switch from its default mode into integration mode, where test software can control directly the inputs and outputs of the PE, for integration testing or topology detection.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

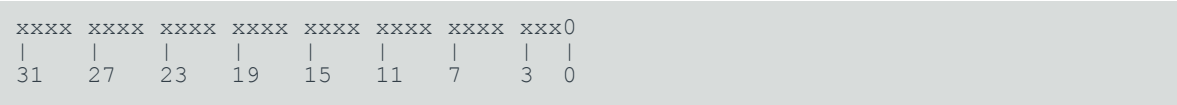
Register offset

0xF00

Access type

See bit descriptions

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-372: EXT\_CTIITCTRL bit assignments

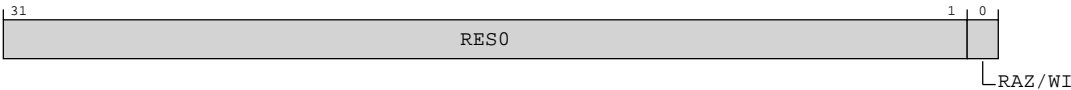


Table B-723: CTIITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Instance	Range
CTI	0xF00	CTIITCTRL	None

This interface is accessible as follows:

**When IsCorePowered() and !OSLockStatus()**

RW

**Otherwise**

ImplementationDefined

B.2.2.6.16 CTICLAIMSET, CTI Claim Tag Set register

Used by software to set CLAIM bits to 1.

Configurations

This register is available in all configurations.

Attributes

**Width**

32

**Component**

CTI

**Register offset**

0xFA0

**Access type**

RAOW1S

**Reset value**

0000 0000 0000 0000 0000 0000 0000 1111

Bit descriptions

Figure B-373: EXT\_CTICLAIMSET bit assignments

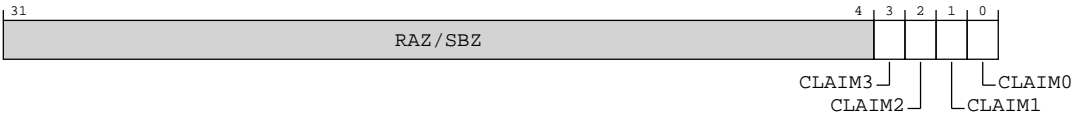


Table B-725: CTICLAIMSET bit descriptions

Bits	Name	Description	Reset
[31:4]	RAZ/SBZ	Reserved	RAZ/SBZ

Bits	Name	Description	Reset
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	<div>CLAIM tag set bit.</div> <div>The bit is <b>RAO</b> and the behavior on writes is:</div> <div><b>0b0</b> No action.</div> <div><b>0b1</b> Indirectly set claim bit to 1.</div> <div>A single write to CTICLAIMSET can set multiple tags to 1.</div>	0b1111 <sup>30</sup>

Accessibility

Component	Offset	Instance	Range
CTI	0xFA0	CTICLAIMSET	None

This interface is accessible as follows:

RW

B.2.2.6.17 CTICLAIMCLR, CTI Claim Tag Clear register

Used by software to read the values of the CLAIM bits, and to clear these bits to 0.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFA4

Access type

RW1C

Reset value

0000	0000	0000	0000	0000	0000	0000	xxxx
31	27	23	19	15	11	7	3 0

<sup>30</sup> An External Debug reset clears the CLAIM tag bits to 0.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.  
Non-Confidential



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-374: EXT\_CTICLAIMCLR bit assignments

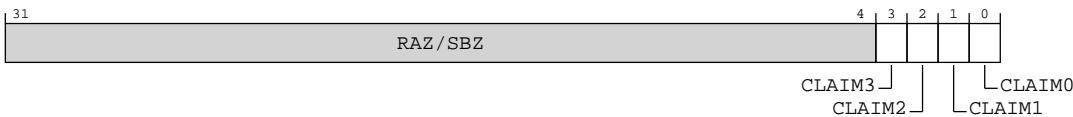


Table B-727: CTICLAIMCLR bit descriptions

Bits	Name	Description	Reset
[31:4]	RAZ/SBZ	Reserved	RAZ/SBZ
[3:0]	CLAIM<x>, bit[x], where x = 3 to 0	CLAIM tag clear bit.  Reads return the value of CLAIM[x] and the behavior on writes is:  <b>0b0</b> No action.  <b>0b1</b> Indirectly clear claim bit to 0.  A single write to CTICLAIMCLR can clear multiple tags to 0.	xxxx <sup>31</sup>

Accessibility

Component	Offset	Instance	Range
CTI	0xFA4	CTICLAIMCLR	None

This interface is accessible as follows:

RW

B.2.2.6.18 CTIDEVAFF0, CTI Device Affinity register 0

Copy of the low half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the CTI component relates to.

Configurations

This register is available in all configurations.

<sup>31</sup> An External Debug reset clears the CLAIM tag bits to 0.

Copyright © 2023–2025 Arm Limited (or its affiliates). All rights reserved.  
Non-Confidential

Attributes

Width

32

Component

CTI

Register offset

0xFA8

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-375: EXT\_CTIDEVAFF0 bit assignments

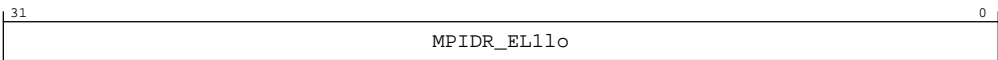


Table B-729: CTIDEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1lo	If the CTI corresponds to a PE, then this field is a read-only copy of the low half of the core's AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.  If the CTI corresponds to the cluster, then this field is a read-only copy of the low half of any of the cores' AArch64-MPIDR_EL1, as seen from the highest implemented Exception level, but with bits [15:8] set to 0x80. In other words, the Aff1 field points to the cluster level, instead of a specific core in the cluster.	32 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0xFA8	CTIDEVAFF0	None

This interface is accessible as follows:

RO

B.2.2.6.19 CTIDEVAFF1, CTI Device Affinity register 1

Copy of the high half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the CTI component relates to.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFAC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-376: EXT\_CTIDEVAFF1 bit assignments

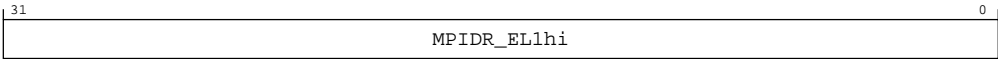


Table B-731: CTIDEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1hi	<p>If the CTI corresponds to a PE, then this field is a read-only copy of the high half of the core's AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.</p> <p>If the CTI corresponds to the cluster, then this field is a read-only copy of the high half of any of the cores' AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.</p>	32 {x}

Accessibility

Component	Offset	Instance	Range
CTI	0xFAC	CTIDEVAFF1	None

This interface is accessible as follows:

RO

B.2.2.6.20 CTILAR, CTI Lock Access Register

Allows or disallows access to the CTI registers through a memory-mapped interface.

The optional Software Lock provides a lock to prevent memory-mapped writes to the Cross-Trigger Interface registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the Cross-Trigger Interface registers. It does not, and cannot, prevent all accidental or malicious damage.

Configurations

Software Lock is not implemented.

Attributes

Width

32

Component

CTI

Register offset

0xFB0

Access type

RESERVEDW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Otherwise



Figure B-377: EXT\_CTILAR bit assignments

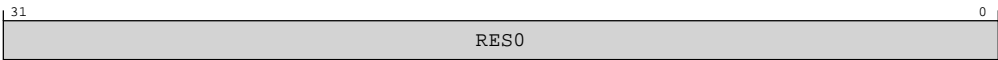


Table B-733: CTILAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
CTI	0xFB0	CTILAR	None

This interface is accessible as follows:

WO

B.2.2.6.21 CTILSR, CTI Lock Status Register

Indicates the current status of the Software Lock for CTI registers.

The optional Software Lock provides a lock to prevent memory-mapped writes to the Cross-Trigger Interface registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the Cross-Trigger Interface registers. It does not, and cannot, prevent all accidental or malicious damage.

Configurations

Software Lock is not implemented.

Attributes

Width

32

Component

CTI

Register offset

0xFB4

Access type

RO

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-378: EXT\_CTILSR bit assignments

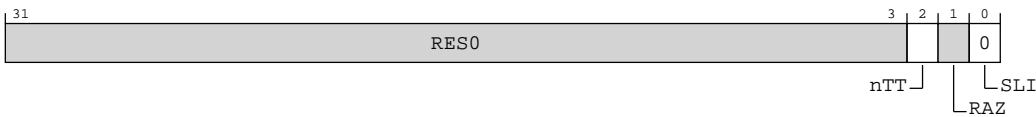


Table B-735: CTILSR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	nTT	Not thirty-two bit access required. <b>RAZ</b> .	x
[1]	RAZ	Reserved	RAZ
[0]	SLI	Software Lock implemented. <b>0b0</b> Software Lock not implemented or not memory-mapped access.	0b0

Accessibility

Component	Offset	Instance	Range
CTI	0xFB4	CTILSR	None

This interface is accessible as follows:

RO

B.2.2.6.22 CTIAUTHSTATUS, CTI Authentication Status register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for CTI.

Configurations

This register is **OPTIONAL**, and is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFB8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-379: EXT\_CTIAUTHSTATUS bit assignments

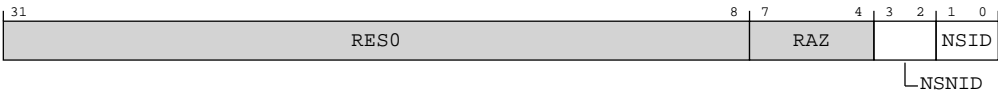


Table B-737: CTIAUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	RAZ	Reserved	RAZ
[3:2]	NSNID	This field holds the same value as ext-DBGAUTHSTATUS_EL1.SNID.	xx
[1:0]	NSID	This field holds the same value as ext-DBGAUTHSTATUS_EL1.SID.	xx

Accessibility

Component	Offset	Instance	Range
CTI	0xFB8	CTIAUTHSTATUS	None

This interface is accessible as follows:

RO

B.2.2.6.23 CTIDEVARCH, CTI Device Architecture register

Identifies the programmers' model architecture of the CTI component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFBC

Access type

RO

Reset value

0100 0111 0111 0001 0001 1010 0001 0100

Bit descriptions

Figure B-380: EXT\_CTIDEVARCH bit assignments

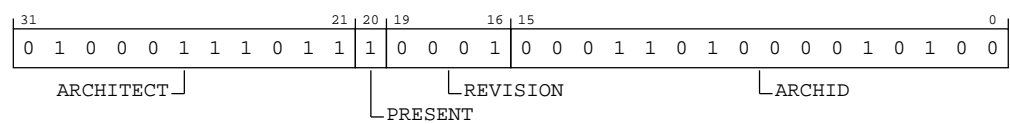


Table B-739: CTIDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Defines the architecture of the component. For CTI, this is Arm Limited.  Bits [31:28] are the JEP106 continuation code, 0x4.  Bits [27:21] are the JEP106 ID code, 0x3B.  <b>0b01000111011</b>	0b01000111011
[20]	PRESENT	Indicates that the DEVARCH is present.  <b>0b1</b>	0b1
[19:16]	REVISION	Revision.  Defines the architecture revision of the component.  <b>0b0001</b> First revision, and also adds support for ext-CTIDEVCTL.  All other values are reserved.	0b0001

Bits	Name	Description	Reset
[15:0]	ARCHID	<div>Defines this part to be an Armv8 debug component. For architectures defined by Arm this is further subdivided.</div> <div>For CTI:</div> <ul style="list-style-type: none"><li>Bits [15:12] are the architecture version, 0x1.</li><li>Bits [11:0] are the architecture part number, 0xA14.</li></ul> <div>This corresponds to CTI architecture version CTIv2.</div> <div>0b0001101000010100</div>	0xA14

Accessibility

Component	Offset	Instance	Range
CTI	0xFBC	CTIDEVARCH	None

This interface is accessible as follows:

RO

B.2.2.6.24 CTIDEVID2, CTI Device ID register 2

Reserved for future information about the CTI component to the debugger.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFC0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-381: EXT\_CTIDEVID2 bit assignments

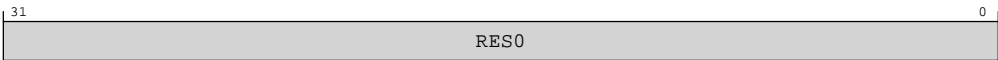


Table B-741: CTIDEVID2 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
CTI	0xFC0	CTIDEVID2	None

This interface is accessible as follows:

RO

B.2.2.6.25 CTIDEVID1, CTI Device ID register 1

Reserved for future information about the CTI component to the debugger.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

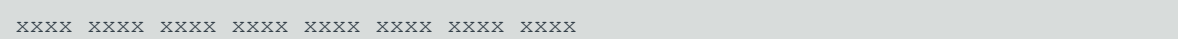
Register offset

0xFC4

Access type

RO

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-382: EXT\_CTIDEVID1 bit assignments

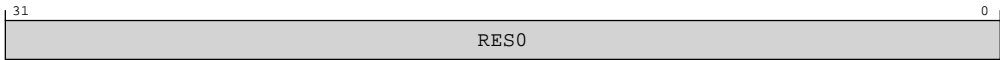


Table B-743: CTIDEVID1 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
CTI	0xFC4	CTIDEVID1	None

This interface is accessible as follows:

RO

B.2.2.6.26 CTIDEVID, CTI Device ID register 0

Describes the CTI component to the debugger.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFC8

Access type

RO

Reset value

xxxx	xx01	xx01	0000	xx00	1010	xxx0	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-383: EXT\_CTIDEVID bit assignments

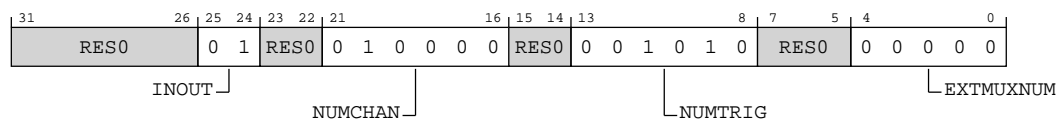


Table B-745: CTIDEVID bit descriptions

Bits	Name	Description	Reset
[31:26]	RES0	Reserved	RES0
[25:24]	INOUT	Input/output options. Indicates presence of the input gate. If the CTM is not implemented or CTIv2 is not implemented, this field is <b>RAZ</b> .  <b>0b01</b> ext-CTIGATE masks propagation of input events from external channels.  All other values are reserved.	0b01
[23:22]	RES0	Reserved	RES0
[21:16]	NUMCHAN	Number of ECT channels implemented.  <b>0b010000</b> 16 channels (0..15) implemented.	0b010000
[15:14]	RES0	Reserved	RES0
[13:8]	NUMTRIG	Number of triggers implemented.  <b>0b001010</b> 10 triggers (0..9) implemented.	0b001010
[7:5]	RES0	Reserved	RES0
[4:0]	EXTMUXNUM	Number of multiplexors available on triggers. This value is used in conjunction with External Control register, ext-ASICCTL.  <b>0b00000</b> No multiplexors implemented. ext-ASICCTL is unused.	0b00000

Accessibility

Component	Offset	Instance	Range
CTI	0xFC8	CTIDEVID	None



This interface is accessible as follows:

RO

B.2.2.6.27 CTIDEVTYPE, CTI Device Type register

Indicates to a debugger that this component is part of a PE's cross-trigger interface.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

CTI

Register offset

0xFCC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-384: EXT\_CTIDEVTYPE bit assignments

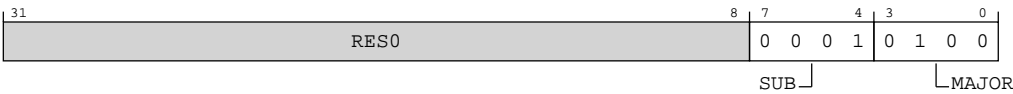


Table B-747: CTIDEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	SUB	Subtype. Indicates this is a component within a PE.  <b>0b0001</b>	0b0001
[3:0]	MAJOR	Major type. Indicates this is a cross-trigger component.  <b>0b0100</b>	0b0100

Accessibility

Component	Offset	Instance	Range
CTI	0xFCC	CTIDEVTYPE	None

This interface is accessible as follows:

RO

B.2.2.6.28 CTIPIDR4, CTI Peripheral Identification Register 4

Provides information to identify a CTI component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFD0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0100
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-385: EXT\_CTIPIDR4 bit assignments

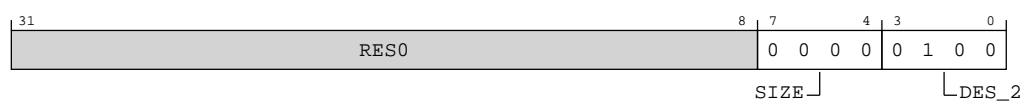


Table B-749: CTIPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	Size of the component. <b>RAZ</b> . Log <sub>2</sub> of the number of 4KB pages from the start of the component to the end of the component ID registers. <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	Designer, JEP106 continuation code, least significant nibble. For Arm Limited, this field is 0b0100. <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Instance	Range
CTI	0xFD0	CTIPIDR4	None

This interface is accessible as follows:

RO

B.2.2.6.29 CTIPIDR0, CTI Peripheral Identification Register 0

Provides information to identify a CTI component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFE0

Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-386: EXT\_CTIPIDR0 bit assignments



Table B-751: CTIPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0]. <b>0b00010100</b> Cortex-R82AE CTI. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Instance	Range
CTI	0xFEO	CTIPIDR0	None

This interface is accessible as follows:

RO

B.2.2.6.30 CTIPIDR1, CTI Peripheral Identification Register 1

Provides information to identify a CTI component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

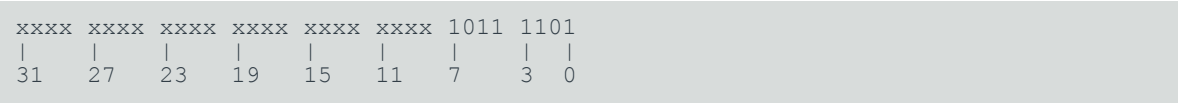
Register offset

0xFE4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-387: EXT\_CTIPIDR1 bit assignments



Table B-753: CTIPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	Designer, least significant nibble of JEP106 ID code. For Arm Limited, this field is 0b1011. <b>0b1011</b> Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8]. <b>0b1101</b> Cortex-R82AE CTI. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Instance	Range
CTI	0xFE4	CTIPIDR1	None

This interface is accessible as follows:

RO

B.2.2.6.31 CTIPIDR2, CTI Peripheral Identification Register 2

Provides information to identify a CTI component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

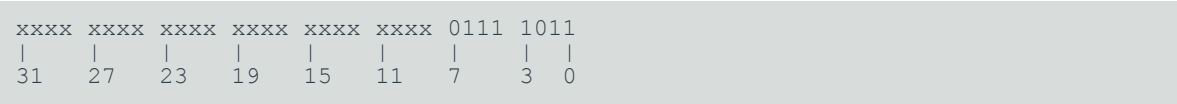
Register offset

0xFE8

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-388: EXT\_CTIPIDR2 bit assignments

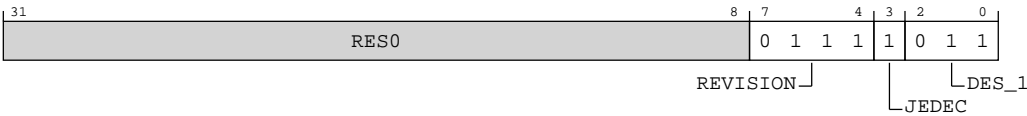


Table B-755: CTIPIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	REVISION	Component revision.  <b>0b0111</b> Revision 7.	0b0111
[3]	JEDEC	<b>RAO</b> . Indicates a JEP106 identity code is used.  <b>0b1</b> JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  <b>0b011</b> Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Instance	Range
CTI	0xFE8	CTIPIDR2	None

This interface is accessible as follows:

RO

B.2.2.6.32 CTIPIDR3, CTI Peripheral Identification Register 3

Provides information to identify a CTI component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFEC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-389: EXT\_CTIPIDR3 bit assignments



Table B-757: CTIPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Part minor revision. Parts using ext-CTIPIDR2.REVISION as an extension to the Part number must use this field as a major revision number.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer modified. Indicates someone other than the Designer has modified the component.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Instance	Range
CTI	0xFEC	CTIPIDR3	None

This interface is accessible as follows:

RO

B.2.2.6.33 CTICIDR0, CTI Component Identification Register 0

Provides information to identify a CTI component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.



Attributes

Width

32

Component

CTI

Register offset

0xFF0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-390: EXT\_CTICIDR0 bit assignments



Table B-759: CTICIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble. <b>0b00001101</b> CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Instance	Range
CTI	0xFF0	CTICIDR0	None

This interface is accessible as follows:

RO

B.2.2.6.34 CTICIDR1, CTI Component Identification Register 1

Provides information to identify a CTI component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFF4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-391: EXT\_CTICIDR1 bit assignments

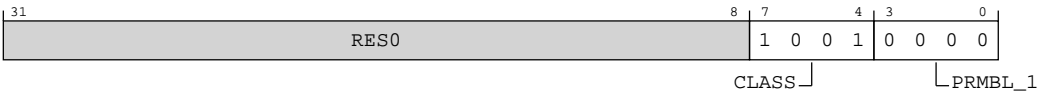


Table B-761: CTICIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	Component class.  <b>0b1001</b> CoreSight debug component.	0b1001

Bits	Name	Description	Reset
[3:0]	PRMBL_1	Preamble.  <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Instance	Range
CTI	0xFF4	CTICIDR1	None

This interface is accessible as follows:

RO

B.2.2.6.35 CTICIDR2, CTI Component Identification Register 2

Provides information to identify a CTI component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFF8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-392: EXT\_CTICIDR2 bit assignments



Table B-763: CTICIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble.  0b00000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Instance	Range
CTI	0xFF8	CTICIDR2	None

This interface is accessible as follows:

RO

B.2.2.6.36 CTICIDR3, CTI Component Identification Register 3

Provides information to identify a CTI component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is required for CoreSight compliance.

Attributes

Width

32

Component

CTI

Register offset

0xFFC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-393: EXT\_CTICIDR3 bit assignments



Table B-765: CTICIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble.  0b10110001 CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Instance	Range
CTI	0xFFC	CTICIDR3	None

This interface is accessible as follows:

RO

B.2.2.7 External ETM register description

This section includes the register descriptions for all memory-mapped *Embedded Trace Macrocell* (ETM) registers that are accessed for each core.

B.2.2.7.1 TRCPRGCTLR, Programming Control Register

Enables the trace unit.

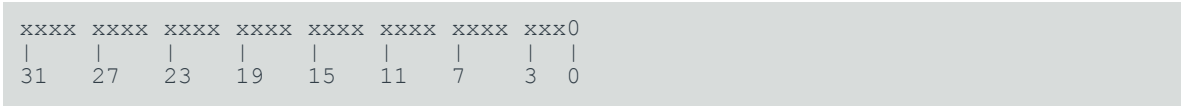
Configurations

External register TRCPRGCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.9 TRCPRGCTLR, Programming Control Register](#) on page 1281 bits [31:0].

Attributes

- Width
- 32
- Component
- ETM
- Register offset
- 0x004
- Access type
- Read
- R
- Write
- W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-394: EXT\_TRCPRGCTLR bit assignments

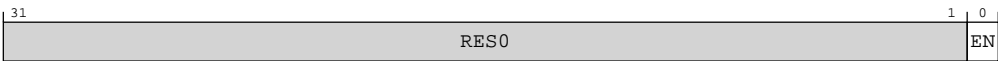


Table B-767: TRCPRGCTLR bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	EN	Trace unit enable.  <b>0b0</b> The trace unit is disabled.  <b>0b1</b> The trace unit is enabled.	0b0

Accessibility

Must be programmed.

Component	Offset	Range
ETM	0x004	None

This interface is accessible as follows:

RW

B.2.2.7.2 TRCSTATR, Trace Status Register

Returns the trace unit status.

Configurations

External register TRCSTATR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.14 TRCSTATR, Trace Status Register](#) on page 1290 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x00C

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-395: EXT\_TRCSTATR bit assignments

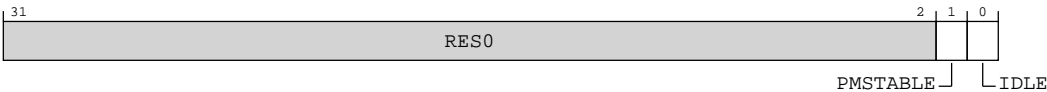


Table B-769: TRCSTATR bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0
[1]	PMSTABLE	Programmers' model stable.  0b0 The programmers' model is not stable.  0b1 The programmers' model is stable.  This bit is <b>UNKNOWN</b> while the trace unit is enabled.	x
[0]	IDLE	Idle status.  0b0 The trace unit is not idle.  0b1 The trace unit is idle.	x

Accessibility

Component	Offset	Range
ETM	0x00C	None

This interface is accessible as follows:

RO

B.2.2.7.3 TRCCONFIGR, Trace Configuration Register

Controls the tracing options.

Configurations

External register TRCCONFIGR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.16 TRCCONFIGR, Trace Configuration Register](#) on page 1293 bits [31:0].

Attributes

Width

32



Component

ETM

Register offset

0x010

Access type

Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-396: EXT\_TRCCONFIGR bit assignments

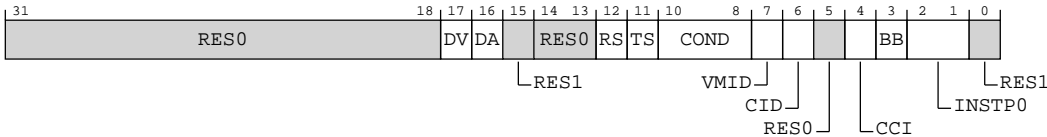


Table B-771: TRCCONFIGR bit descriptions

Bits	Name	Description	Reset
[31:18]	RES0	Reserved	RES0
[17]	DV	Data value tracing bit. <b>0b0</b> Data value tracing is disabled. <b>0b1</b> Data value tracing is enabled when INSTP0 is not 0b00.	x
[16]	DA	Data address tracing bit. <b>0b0</b> Data address tracing is disabled. <b>0b1</b> Data address tracing is enabled when INSTP0 is not 0b00.	x
[15]	RES1	Reserved	RES1

Bits	Name	Description	Reset
[14:13]	<b>RES0</b>	Reserved	<b>RES0</b>
[12]	RS	Return stack control.  <b>0b0</b> Return stack is disabled.  <b>0b1</b> Return stack is enabled.	x
[11]	TS	Global timestamp tracing control.  <b>0b0</b> Global timestamp tracing is disabled.  <b>0b1</b> Global timestamp tracing is enabled.	x
[10:8]	COND	Conditional instruction tracing bit. The permitted values are:  <b>0b000</b> Conditional instruction tracing is disabled.  <b>0b001</b> Conditional load instructions are traced.  <b>0b010</b> Conditional store instructions are traced.  <b>0b011</b> Conditional load and store instructions are traced.  <b>0b111</b> All conditional instructions are traced.	xxx
[7]	VMID	Virtual context identifier tracing control.  <b>0b0</b> Virtual context identifier tracing is disabled.  <b>0b1</b> Virtual context identifier tracing is enabled.	x
[6]	CID	Context identifier tracing control.  <b>0b0</b> Context identifier tracing is disabled.  <b>0b1</b> Context identifier tracing is enabled.	x
[5]	<b>RES0</b>	Reserved	<b>RES0</b>
[4]	CCI	Cycle counting instruction tracing control.  <b>0b0</b> Cycle counting instruction tracing is disabled.  <b>0b1</b> Cycle counting instruction tracing is enabled.	x

Bits	Name	Description	Reset
[3]	BB	Branch broadcasting control.  <b>0b0</b> Branch broadcasting is disabled.  <b>0b1</b> Branch broadcasting is enabled.	x
[2:1]	INSTPO	Instruction PO field. This field controls whether load and store instructions are traced as PO instructions:  <b>0b00</b> Do not trace load and store instructions as PO instructions.  <b>0b01</b> Trace load instructions as PO instructions.  <b>0b10</b> Trace store instructions as PO instructions.  <b>0b11</b> Trace load and store instructions as PO instructions.	xx
[0]	RES1	Reserved	RES1

### Access

Must always be programmed.

TRCCONFIGR.QE must be set to 0b00 if TRCCONFIGR.BB is not 0b0.

### Accessibility

Must always be programmed.

TRCCONFIGR.QE must be set to 0b00 if TRCCONFIGR.BB is not 0b0.

Component	Offset	Range
ETM	0x010	None

This interface is accessible as follows:

RW

#### B.2.2.7.4 TRCAUXCTLR, Auxillary Control Register

Trace micro-architectural control bits.

### Configurations

External register TRCAUXCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.19 TRCAUXCTLR, Auxillary Control Register](#) on page 1300 bits [31:0].

### Attributes

#### Width

32

Component

ETM

Register offset

0x018

Access type

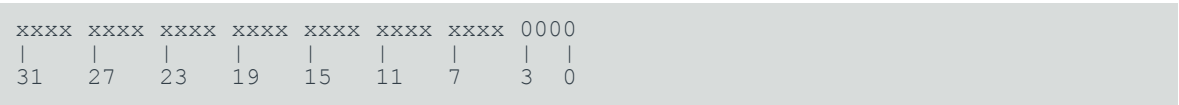
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-397: EXT\_TRCAUXCTLR bit assignments

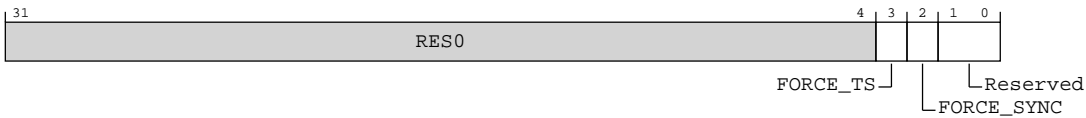


Table B-773: TRCAUXCTLR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3]	FORCE_TS	Force overflow when no timestamp is generated between two trace info packets.  <b>0b0</b> Force overflow disabled.  <b>0b1</b> Force overflow enabled.	0b0
[2]	FORCE_SYNC	Force overflow when the generation of trace synchronisation packets is delayed.  <b>0b0</b> Force overflow disabled.  <b>0b1</b> Force overflow enabled.	0b0

Bits	Name	Description	Reset
[1:0]	Reserved	Trace unit control options which are reserved for Arm internal use.  <b>0b00</b> Any trace unit control options affected by this register are disabled.  All other values are reserved for Arm internal use. Arm strongly recommends that you do not modify this field unless directed by Arm.	0b00

Accessibility

If this register is set to nonzero then it might cause the behavior of a trace unit to contradict the architecture specification. Therefore, Arm strongly recommends that you do not modify this register unless directed by Arm.

Component	Offset	Range
ETM	0x018	None

This interface is accessible as follows:

RW

B.2.2.7.5 TRCEVENTCTLOR, Event Control 0 Register

Controls the generation of tracing events.

Configurations

External register TRCEVENTCTLOR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.22 TRCEVENTCTLOR, Event Control 0 Register](#) on page 1307 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x020

Access type

Read

R

Write

W

Reset value



31 27 23 19 15 11 7 3 0

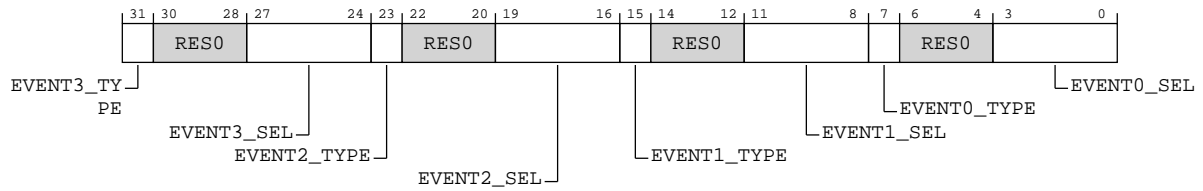


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-398: EXT\_TRCEVENTCTL0R bit assignments**



**Table B-775: TRCEVENTCTL0R bit descriptions**

Bits	Name	Description	Reset
[31]	EVENT3_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENT3_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENT3_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT3_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[30:28]	RES0	Reserved	RES0
[27:24]	EVENT3_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENT3_TYPE controls whether EVENT3_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.  When any of the selected resource events occurs and ext-TRCEVENTCTL1R.INSTEN[3] == 0b1, then Event element 3 is generated in the instruction trace element stream.	xxxx

Bits	Name	Description	Reset
[23]	EVENT2_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT2_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT2_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT2_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[22:20]	RES0	Reserved	RES0
[19:16]	EVENT2_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT2_TYPE controls whether EVENT2_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and ext-TRCEVENTCTL1R.INSTEN[2] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx
[15]	EVENT1_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT1_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT1_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT1_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[14:12]	RES0	Reserved	RES0
[11:8]	EVENT1_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT1_TYPE controls whether EVENT1_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p> <p>When any of the selected resource events occurs and ext-TRCEVENTCTL1R.INSTEN[1] == 0b1, then Event element 3 is generated in the instruction trace element stream.</p>	xxxx

Bits	Name	Description	Reset
[7]	EVENTO_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENTO_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENTO_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENTO_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENTO_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENTO_TYPE controls whether EVENTO_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.  When any of the selected resource events occurs and ext-TRCEVENTCTL1R.INSTEN[0] == 0b1, then Event element 3 is generated in the instruction trace element stream.	xxxx

## Accessibility

Must be programmed if implemented.

Component	Offset	Range
ETM	0x020	None

This interface is accessible as follows:

RW

### B.2.2.7.6 TRCEVENTCTL1R, Event Control 1 Register

Controls the behavior of the tracing events that ext-TRCEVENTCTL0R selects.

## Configurations

External register TRCEVENTCTL1R bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.26 TRCEVENTCTL1R, Event Control 1 Register](#) on page 1318 bits [31:0].

## Attributes

### Width

32

### Component

ETM



Register offset

0x024

Access type

Read

R

Write

W

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-399: EXT\_TRCEVENTCTL1R bit assignments

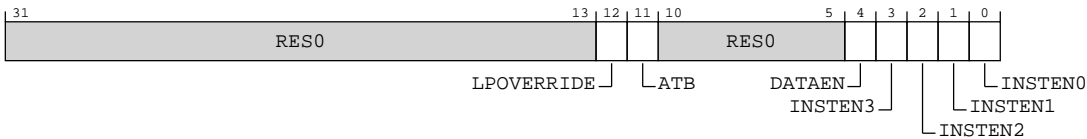


Table B-777: TRCEVENTCTL1R bit descriptions

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0
[12]	LPOVERRIDE	Low-power Override Mode select.  <b>0b0</b> Trace unit Low-power Override Mode is not enabled. That is, the trace unit is permitted to enter low-power state.  <b>0b1</b> Trace unit Low-power Override Mode is enabled. That is, entry to a low-power state does not affect the trace unit resources or trace generation.	x

Bits	Name	Description	Reset
[11]	ATB	<p>AMBA Trace Bus (ATB) trigger enable.</p> <p>When trace event 0 occurs the trace unit sets:</p> <ul style="list-style-type: none"> <li>• ATID == 0x7D.</li> <li>• ATDATA to the value of ext-TRCTRACEIDR.</li> </ul> <p>If the width of ATDATA is greater than the width of ext-TRCTRACEIDR.TRACEID then the trace unit zeros the upper ATDATA bits.</p> <p>If trace event 0 is programmed to occur based on program execution, such as an address comparator, the ATB trigger might not be inserted into the ATB stream at the same time as any trace generated by that program execution is output by the trace unit. Typically, the generated trace might be buffered in a trace unit which means that the ATB trigger would be output before the associated trace is output.</p> <p>If trace event 0 is asserted multiple times in close succession, the trace unit is required to generate an ATB trigger for the first assertion, but might ignore one or more of the subsequent assertions. Arm recommends that the window in which ETMEvent 0 is ignored is limited only by the time taken to output an ATB trigger.</p> <p><b>0b0</b> ATB trigger is disabled.</p> <p><b>0b1</b> ATB trigger is enabled.</p>	x
[10:5]	RES0	Reserved	RES0
[4]	DATAEN	<p>Data event enable bit.</p> <p><b>0b0</b> If event 0 occurs, the trace unit does not generate an Event element.</p> <p><b>0b1</b> If event 0 occurs, the trace unit generates an Event element in the data trace stream.</p>	x
[3:0]	INSTEN<m>, bit[m], where m = 3 to 0	<p>Event element control.</p> <p><b>0b0</b> The trace unit does not generate an Event element m.</p> <p><b>0b1</b> The trace unit generates an Event element m.</p>	xxxx

## Accessibility

Must be programmed.

Component	Offset	Range
ETM	0x024	None

This interface is accessible as follows:

RW

B.2.2.7.7 TRCSTALLCTLR, Stall Control Register

Enables trace unit functionality that prevents trace unit buffer overflows.

Configurations

External register TRCSTALLCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.31 TRCSTALLCTLR, Stall Control Register](#) on page 1330 bits [31:0].

Attributes

**Width**  
32

**Component**  
ETM

**Register offset**  
0x02C

**Access type**  
**Read**  
R  
**Write**  
W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-400: EXT\_TRCSTALLCTLR bit assignments

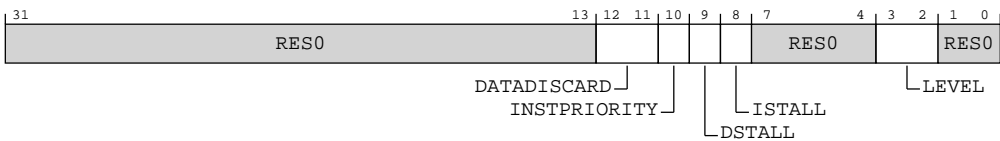


Table B-779: TRCSTALLCTLR bit descriptions

Bits	Name	Description	Reset
[31:13]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[12:11]	DATADISCARD	<p>Data discard field. Controls if a trace unit can discard data trace elements when the data trace buffer space is less than LEVEL.</p> <p><b>0b00</b> The trace unit must not discard any data trace elements.</p> <p><b>0b01</b> The trace unit can discard P1 and P2 elements associated with data loads.</p> <p><b>0b10</b> The trace unit can discard P1 and P2 elements associated with data stores.</p> <p><b>0b11</b> The trace unit can discard P1 and P2 elements associated with both data loads and stores.</p>	xx
[10]	INSTPRIORITY	<p>Prioritize instruction trace bit. Controls if a trace unit can prioritize instruction trace when the instruction trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not prioritize instruction trace.</p> <p><b>0b1</b> The trace unit can prioritize instruction trace. A trace unit might prioritize</p>	x
[9]	DSTALL	<p>Data stall bit. Controls if a trace unit can stall the PE when the data trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not stall the PE.</p> <p><b>0b1</b> The trace unit can stall the PE.</p>	x
[8]	ISTALL	<p>Instruction stall control. Controls if a trace unit can stall the PE when the trace buffer space is less than LEVEL.</p> <p><b>0b0</b> The trace unit must not stall the PE.</p> <p><b>0b1</b> The trace unit can stall the PE.</p>	x
[7:4]	RES0	Reserved	RES0
[3:2]	LEVEL	<p>Threshold level field. The field supports 4 monotonic levels from 0b00 to 0b11.</p> <p><b>0b00</b> Minimal invasion. This setting has a greater risk of a trace unit buffer overflow.</p> <p><b>0b01</b> Small invasion.</p> <p><b>0b10</b> Big invasion.</p> <p><b>0b11</b> Maximum invasion. Reduced risk of a trace unit buffer overflow.</p>	xx
[1:0]	RES0	Reserved	RES0

## Accessibility

Must be programmed if implemented.

Component	Offset	Range
ETM	0x02C	None

This interface is accessible as follows:

RW

B.2.2.7.8 TRCTSCTLR, Timestamp Control Register

Controls the insertion of global timestamps in the trace stream.

Configurations

External register TRCTSCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.33 TRCTSCTLR, Timestamp Control Register](#) on page 1336 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x030

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-401: EXT\_TRCTSCTLR bit assignments

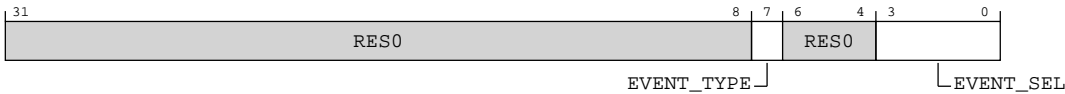


Table B-781: TRCTSCTLR bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7]	EVENT_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

Accessibility

Must be programmed if ext-TRCCONFIGR.TS == 0b1.

Component	Offset	Range
ETM	0x030	None

This interface is accessible as follows:

RW

B.2.2.7.9 TRCSYNCP, Synchronization Period Register

Controls how often trace protocol synchronization requests occur.

Configurations

External register TRCSYNCP bits [31:0] are architecturally mapped to AArch64 System register A.2.8.35 TRCSYNCP, Synchronization Period Register on page 1340 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x034

Access type

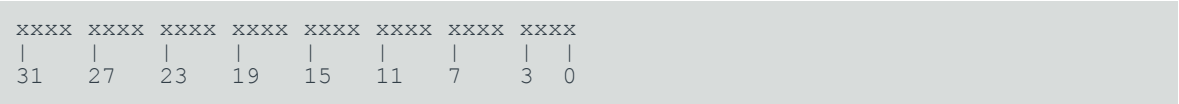
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-402: EXT\_TRCSYNCPR bit assignments

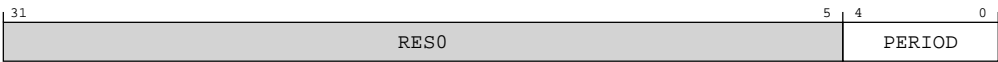


Table B-783: TRCSYNCPR bit descriptions

Bits	Name	Description	Reset
[31:5]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[4:0]	PERIOD	<p>Defines the number of bytes of trace between each periodic trace protocol synchronization request.</p> <p><b>0b000000</b> Trace protocol synchronization is disabled.</p> <p><b>0b010000</b> Trace protocol synchronization request occurs after <math>2^8</math> bytes of trace.</p> <p><b>0b01001</b> Trace protocol synchronization request occurs after <math>2^9</math> bytes of trace.</p> <p><b>0b01010</b> Trace protocol synchronization request occurs after <math>2^{10}</math> bytes of trace.</p> <p><b>0b01011</b> Trace protocol synchronization request occurs after <math>2^{11}</math> bytes of trace.</p> <p><b>0b01100</b> Trace protocol synchronization request occurs after <math>2^{12}</math> bytes of trace.</p> <p><b>0b01101</b> Trace protocol synchronization request occurs after <math>2^{13}</math> bytes of trace.</p> <p><b>0b01110</b> Trace protocol synchronization request occurs after <math>2^{14}</math> bytes of trace.</p> <p><b>0b01111</b> Trace protocol synchronization request occurs after <math>2^{15}</math> bytes of trace.</p> <p><b>0b10000</b> Trace protocol synchronization request occurs after <math>2^{16}</math> bytes of trace.</p> <p><b>0b10001</b> Trace protocol synchronization request occurs after <math>2^{17}</math> bytes of trace.</p> <p><b>0b10010</b> Trace protocol synchronization request occurs after <math>2^{18}</math> bytes of trace.</p> <p><b>0b10011</b> Trace protocol synchronization request occurs after <math>2^{19}</math> bytes of trace.</p> <p><b>0b10100</b> Trace protocol synchronization request occurs after <math>2^{20}</math> bytes of trace.</p> <p>Other values are reserved. If a reserved value is programmed into PERIOD, then one of the following behaviors occurs:</p> <ul style="list-style-type: none"> <li>If a reserved value less than 0b01000 is programmed, trace protocol synchronisation requests occur at approximately the specified period.</li> <li>If a reserved value greater than 0b10100 is programmed, no trace protocol synchronisation requests are generated.</li> </ul>	5 {x}

## Accessibility

Must be programmed if ext-TRCIDR3.SYNCPR == 0b0.

Component	Offset	Range
ETM	0x034	None

This interface is accessible as follows:



RW

B.2.2.7.10 TRCCCCTLR, Cycle Count Control Register

Set the threshold value for cycle counting.

Configurations

External register TRCCCCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.37 TRCCCCTLR, Cycle Count Control Register](#) on page 1345 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x038

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-403: EXT\_TRCCCCTLR bit assignments



**Table B-785: TRCCCCTLR bit descriptions**

Bits	Name	Description	Reset
[31:12]	RES0	Reserved	RES0
[11:0]	THRESHOLD	<p>Sets the threshold value for instruction trace cycle counting.</p> <p>The minimum threshold value that can be programmed into THRESHOLD is given in ext-TRCIDR3.CCITMIN. If the THRESHOLD value is smaller than the value in ext-TRCIDR3.CCITMIN, then no cycle counts are generated in the trace and the cycle count threshold is not included in a traceinfo packet.</p> <p>Writing a value of zero when ext-TRCCONFIGR.CCI is set to enable instruction trace cycle counting, then no cycle counts are generated in the trace and the cycle count threshold is not included in a traceinfo packet.</p>	12 {x}

### Accessibility

Must be programmed if ext-TRCCONFIGR.CCI == 0b1.

Component	Offset	Range
ETM	0x038	None

This interface is accessible as follows:

RW

#### B.2.2.7.11 TRCBBCTLR, Branch Broadcast Control Register

Controls the regions in the memory map where branch broadcasting is active.

### Configurations

External register TRCBBCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.39 TRCBBCTLR, Branch Broadcast Control Register](#) on page 1349 bits [31:0].

### Attributes

#### Width

32

#### Component

ETM

#### Register offset

0x03C

#### Access type

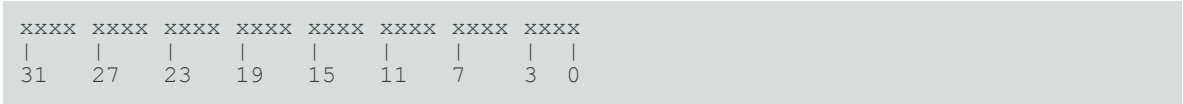
##### Read

R

##### Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-404: EXT\_TRCBBCTLR bit assignments

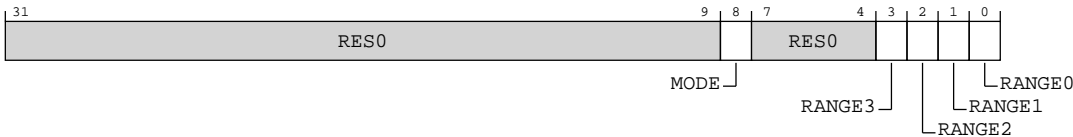


Table B-787: TRCBBCTLR bit descriptions

Bits	Name	Description	Reset
[31:9]	RES0	Reserved	RES0
[8]	MODE	Mode.  <b>0b0</b> Exclude Mode.  Branch broadcasting is not active for instructions in the address ranges defined by RANGE.  If RANGE == 0x00 then branch broadcasting is active for all instructions.  <b>0b1</b> Include Mode.  Branch broadcasting is active for instructions in the address ranges defined by RANGE.  If RANGE == 0x00 then no instructions are considered to be in the branch broadcasting region.	x
[7:4]	RES0	Reserved	RES0
[3:0]	RANGE<m>, bit[m], where m = 3 to 0	Address range field.  Selects which Address Range Comparators are in use with branch broadcasting.  <b>0b0</b> The address range that Address Range Comparator m defines, is not selected.  <b>0b1</b> The address range that Address Range Comparator m defines, is selected.	xxxx

Accessibility

Must be programmed if ext-TRCCONFIGR.BB == 0b1.

Component	Offset	Range
ETM	0x03C	None

This interface is accessible as follows:

RW

B.2.2.7.12 TRCTRACEIDR, Trace ID Register

Sets the trace ID for instruction trace.

Configurations

External register TRCTRACEIDR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.5 TRCTRACEIDR, Trace ID Register](#) on page 1271 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x040

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-405: EXT\_TRCTRACEIDR bit assignments

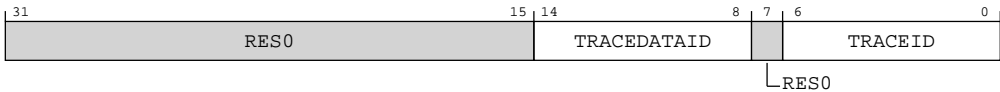


Table B-789: TRCTRACEIDR bit descriptions

Bits	Name	Description	Reset
[31:15]	RES0	Reserved	RES0
[14:8]	TRACEDATAID	<p>Data Trace ID.</p> <p>Sets the trace ID value for data trace.</p> <p>Writing a reserved trace ID value does not affect behavior of the trace unit but it might cause <b>UNPREDICTABLE</b> behavior of the trace capture infrastructure.</p> <p>See the AMBA ATB Protocol Specification for information about which ATID values are reserved.</p>	7 {x}
[7]	RES0	Reserved	RES0
[6:0]	TRACEID	<p>Trace ID.</p> <p>Sets the trace ID value for instruction trace.</p> <p>Writing a reserved trace ID value does not affect behavior of the trace unit but it might cause <b>UNPREDICTABLE</b> behavior of the trace capture infrastructure.</p> <p>See the AMBA ATB Protocol Specification for information about which ATID values are reserved.</p>	7 {x}

Accessibility

Must be programmed if implemented.

Component	Offset	Range
ETM	0x040	None

This interface is accessible as follows:

RW

B.2.2.7.13 TRCVICTLR, ViewInst Main Control Register

Controls instruction trace filtering.

Configurations

External register TRCVICTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.6 TRCVICTLR, ViewInst Main Control Register](#) on page 1274 bits [31:0].

Attributes

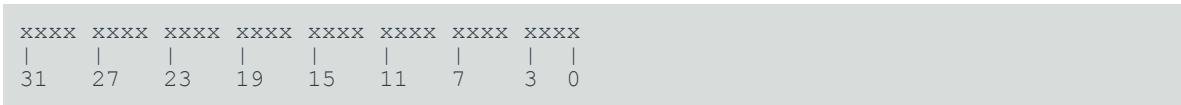
Width  
32

Component  
ETM

Register offset  
0x080

Access type  
Read  
R  
Write  
W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-406: EXT\_TRCVICTLR bit assignments

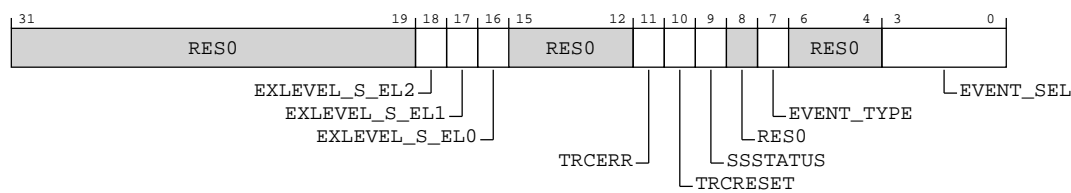


Table B-791: TRCVICTLR bit descriptions

Bits	Name	Description	Reset
[31:19]	RES0	Reserved	RES0
[18]	EXLEVEL_S_EL2	Filter instruction trace for EL2 in Secure state. <b>0b0</b> The trace unit generates instruction trace for EL2 in Secure state. <b>0b1</b> The trace unit does not generate instruction trace for EL2 in Secure state.	x

Bits	Name	Description	Reset
[17]	EXLEVEL_S_EL1	Filter instruction trace for EL1 in Secure state.  <b>0b0</b> The trace unit generates instruction trace for EL1 in Secure state.  <b>0b1</b> The trace unit does not generate instruction trace for EL1 in Secure state.	x
[16]	EXLEVEL_S_ELO	Filter instruction trace for ELO in Secure state.  <b>0b0</b> The trace unit generates instruction trace for ELO in Secure state.  <b>0b1</b> The trace unit does not generate instruction trace for ELO in Secure state.	x
[15:12]	RES0	Reserved	RES0
[11]	TRCERR	Controls the forced tracing of System Error exceptions.  <b>0b0</b> Forced tracing of System Error exceptions is disabled.  <b>0b1</b> Forced tracing of System Error exceptions is enabled.	x
[10]	TRCRESET	Controls the forced tracing of PE Resets.  <b>0b0</b> Forced tracing of PE Resets is disabled.  <b>0b1</b> Forced tracing of PE Resets is enabled.	x
[9]	SSSTATUS	ViewInst start/stop function status.  <b>0b0</b> Stopped State.  The ViewInst start/stop function is in the stopped state.  <b>0b1</b> Started State.  The ViewInst start/stop function is in the started state.  Before software enables the trace unit, it must write to this bit to set the initial state of the ViewInst start/stop function. If the ViewInst start/stop function is not used then set this bit to 0b1. Arm recommends that the value of this bit is set before each trace session begins.  If the trace unit becomes disabled while a start point or stop point is still speculative, then the value of SSSTATUS is <b>UNKNOWN</b> and might represent the result of a speculative start point or stop point.  If software which is running on the PE being traced disables the trace unit, either by clearing ext-TRCPRGCTLR.EN or locking the OS Lock, Arm recommends that a DSB and an ISB instruction are executed before disabling the trace unit to prevent any start points or stop points being speculative at the point of disabling the trace unit. This procedure assumes that all start points or stop points occur before the barrier instructions are executed. The procedure does not guarantee that there are no speculative start points or stop points when disabling, although it helps minimize the probability.	x
[8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7]	EVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

## Accessibility

Must be programmed.

Component	Offset	Range
ETM	0x080	None

This interface is accessible as follows:

RW

### B.2.2.7.14 TRCVIIECTLR, ViewInst Include/Exclude Control Register

Use this to select, or read, the Address Range Comparators for the ViewInst include/exclude function.

## Configurations

External register TRCVIIECTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.10 TRCVIIECTLR, ViewInst Include/Exclude Control Register](#) on page 1283 bits [31:0].

## Attributes

### Width

32

### Component

ETM

### Register offset

0x084



Access type

Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-407: EXT\_TRCVIIECTLR bit assignments

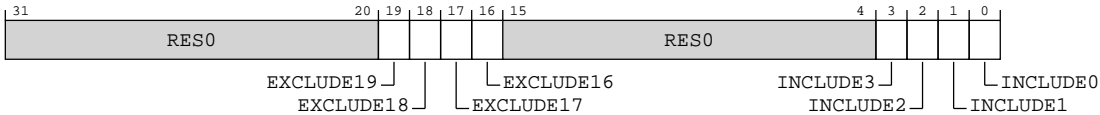


Table B-793: TRCVIIECTLR bit descriptions

Bits	Name	Description	Reset
[31:20]	RES0	Reserved	RES0
[19:16]	EXCLUDE<m>, bit[m], where m = 19 to 16	<p>Selects which Address Range Comparators are in use with the ViewInst exclude function.</p> <p>Each bit represents an Address Range Comparator, so bit[m] controls the selection of Address Range Comparator m.</p> <p><b>0b0</b></p> <p>The address range that Address Range Comparator m defines, is not selected for the ViewInst exclude function.</p> <p><b>0b1</b></p> <p>The address range that Address Range Comparator m defines, is selected for the ViewInst exclude function.</p>	xxxx
[15:4]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[3:0]	INCLUDE<m>, bit[m], where m = 3 to 0	<p>Selects which Address Range Comparators are in use with the ViewInst include function.</p> <p>Each bit represents an Address Range Comparator, so bit[m] controls the selection of Address Range Comparator m.</p> <p>Selecting no comparators for the ViewInst include function indicates that all instructions are included by default.</p> <p>The ViewInst exclude function then indicates which ranges are excluded.</p> <p><b>0b0</b></p> <p>The address range that Address Range Comparator m defines, is not selected for the ViewInst include function.</p> <p><b>0b1</b></p> <p>The address range that Address Range Comparator m defines, is selected for the ViewInst include function.</p>	xxxx

### Accessibility

Must be programmed if ext-TRCIDR4.NUMACPAIRS > 0b0000.

Component	Offset	Range
ETM	0x084	None

This interface is accessible as follows:

RW

#### B.2.2.7.15 TRCVISSCTLR, ViewInst Start/Stop Control Register

Use this to select, or read, the Single Address Comparators for the ViewInst start/stop function.

### Configurations

External register TRCVISSCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.12 TRCVISSCTLR, ViewInst Start/Stop Control Register](#) on page 1286 bits [31:0].

### Attributes

#### Width

32

#### Component

ETM

#### Register offset

0x088

#### Access type

Read

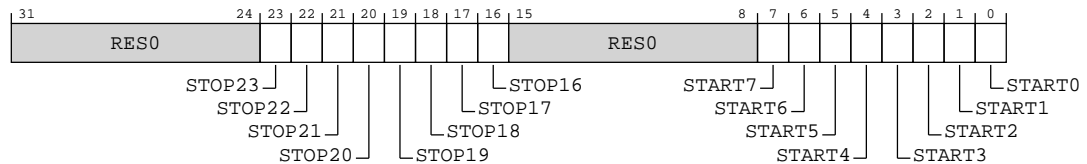
R

**Write**

W

**Reset value****Note**

Where the reset reads xxxx, see individual bits.

**Bit descriptions****Figure B-408: EXT\_TRCVISSCTLR bit assignments****Table B-795: TRCVISSCTLR bit descriptions**

Bits	Name	Description	Reset
[31:24]	RES0	Reserved	RES0
[23:16]	STOP<m>, bit[m], where m = 23 to 16	<p>Selects which Single Address Comparators are in use with ViewInst start/stop function, for the purpose of stopping trace.</p> <p><b>0b0</b> The Single Address Comparator m, is not selected as a stop resource.</p> <p><b>0b1</b> The Single Address Comparator m, is selected as a stop resource.</p>	8 {x}
[15:8]	RES0	Reserved	RES0
[7:0]	START<m>, bit[m], where m = 7 to 0	<p>Selects which Single Address Comparators are in use with ViewInst start/stop function, for the purpose of starting trace.</p> <p><b>0b0</b> The Single Address Comparator m, is not selected as a start resource.</p> <p><b>0b1</b> The Single Address Comparator m, is selected as a start resource.</p>	8 {x}

**Access**

Must be programmed if ext-TRCIDR4.NUMACPAIRS &gt; 0b0000.

For any 2 comparators selected for the ViewInst start/stop function, the comparator containing the lower address must be a lower numbered comparator.

Accessibility

Must be programmed if ext-TRCIDR4.NUMACPAIRS > 0b0000.

For any 2 comparators selected for the ViewInst start/stop function, the comparator containing the lower address must be a lower numbered comparator.

Component	Offset	Range
ETM	0x088	None

This interface is accessible as follows:

RW

B.2.2.7.16 TRCVDCTLR, ViewData Main Control Register

Controls data trace filtering.

Configurations

External register TRCVDCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.23 TRCVDCTLR, ViewData Main Control Register](#) on page 1310 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x0A0

Access type

Read

R

Write

W

Reset value

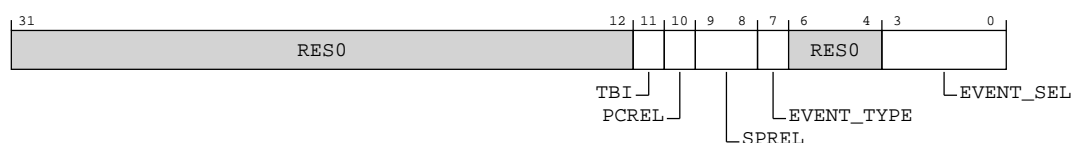
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure B-409: EXT\_TRCVDCTLR bit assignments



### Table B-797: TRCVDCTLR bit descriptions

Bits	Name	Description	Reset
[31:12]	RES0	Reserved	RES0
[11]	TBI	Controls which information a trace unit populates in bits[63:56] of the data address.  <b>0b0</b> The trace unit assigns bits[63:56] to have the same value as bit[55] of the data address, that is, it sign-extends the value.  <b>0b1</b> The trace unit assigns bits[63:56] to have the same value as bits[63:56] of the data address.	x
[10]	PCREL	Controls whether a trace unit traces data for transfers that are relative to the Program Counter (PC).  <b>0b0</b> The trace unit does not affect the tracing of PC-relative transfers.  <b>0b1</b> The trace unit does not trace the address or value portions of PC-relative transfers.  This bit only affects PC-relative transfers that use the PC as a base register plus an immediate offset.	x
[9:8]	SPREL	Controls whether a trace unit traces data for transfers that are relative to the Stack Pointer (SP).  <b>0b00</b> The trace unit does not affect the tracing of SP-relative transfers.  <b>0b01</b> Reserved.  <b>0b10</b> The trace unit does not trace the address portion of SP-relative transfers. If data value tracing is enabled then the trace unit generates a P1 data address element.  <b>0b11</b> The trace unit does not trace the address or value portions of SP-relative transfers.	xx

Bits	Name	Description	Reset
[7]	EVENT_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  EVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  EVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. EVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	EVENT_SEL	Defines the selected Resource Selector or pair of Resource Selectors. EVENT_TYPE controls whether EVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

### Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when data tracing is enabled, that is, when either ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.

### Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when data tracing is enabled, that is, when either ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.

Component	Offset	Range
ETM	0x0A0	None

This interface is accessible as follows:

RW

B.2.2.7.17 TRCVDSACCTLR, ViewData Include/Exclude Single Address Comparator Control Register

Use this to select, or read, the Single Address Comparators for the ViewData include/exclude control.

Configurations

External register TRCVDSACCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.27 TRCVDSACCTLR, ViewData Include/Exclude Single Address Comparator Control Register](#) on page 1321 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x0A4

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0

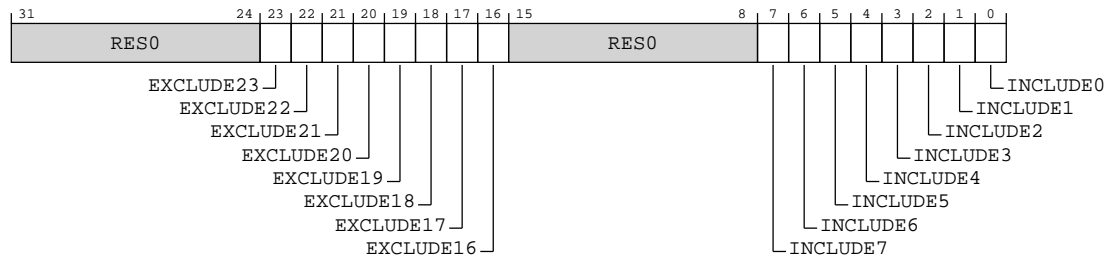


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-410: EXT\_TRCVDSACCTLR bit assignments**



**Table B-799: TRCVDSACCTLR bit descriptions**

Bits	Name	Description	Reset
[31:24]	<b>RES0</b>	Reserved	<b>RES0</b>
[23:16]	EXCLUDE<m>, bit[m], where m = 23 to 16	<p>Selects which single address comparators are in use with ViewData exclude control..</p> <p><b>0b0</b></p> <p>The single address comparator m, is not selected for exclude control.</p> <p><b>0b1</b></p> <p>The single address comparator m, is selected for exclude control.</p>	8 {x}
[15:8]	<b>RES0</b>	Reserved	<b>RES0</b>
[7:0]	INCLUDE<m>, bit[m], where m = 7 to 0	<p>Selects which single address comparators are in use with ViewData include control.</p> <p><b>0b0</b></p> <p>The single address comparator m, is not selected for include control.</p> <p><b>0b1</b></p> <p>The single address comparator m, is selected for include control.</p> <p>If no single address comparators and no address range comparators are selected to be included, then all data transfers are included by default. The exclude control then indicates which data transfers are excluded.</p>	8 {x}

## Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, ext-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects a single address comparator that is either:

- Programmed to be sensitive to a data value comparator.
- Programmed to be an instruction address comparator.



In these situations, data transfers might be traced unexpectedly or might not be traced.

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, ext-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects a single address comparator that is either:

- Programmed to be sensitive to a data value comparator.
- Programmed to be an instruction address comparator.

In these situations, data transfers might be traced unexpectedly or might not be traced.

Component	Offset	Range
ETM	0x0A4	None

This interface is accessible as follows:

RW

B.2.2.7.18 TRCVDARCCTLR, ViewData Include/Exclude Address Range Comparator Control Register

Use this to select, or read, the Address Range Comparator for the ViewData include/exclude control.

Configurations

External register TRCVDARCCTLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.29 TRCVDARCCTLR, ViewData Include/Exclude Address Range Comparator Control Register](#) on page 1325 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x0A8

Access type

Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-411: EXT\_TRCVDARCCTLR bit assignments

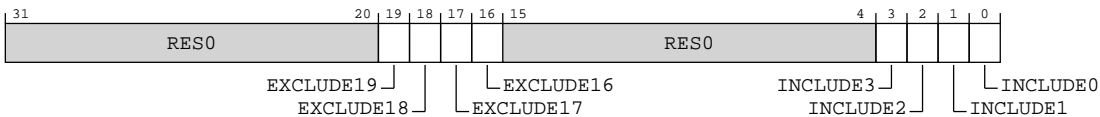


Table B-801: TRCVDARCCTLR bit descriptions

Bits	Name	Description	Reset
[31:20]	RES0	Reserved	RES0
[19:16]	EXCLUDE<m>, bit[m], where m = 19 to 16	<p>Exclude range field. Selects which address range comparator pairs are in use with ViewData exclude control.</p> <p><b>0b0</b></p> <p>The address range that address range comparator pair m defines, is not selected for ViewData exclude control.</p> <p><b>0b1</b></p> <p>The address range that address range comparator pair m defines, is selected for ViewData exclude control.</p>	xxxx
[15:4]	RES0	Reserved	RES0
[3:0]	INCLUDE<m>, bit[m], where m = 3 to 0	<p>Include range field. Selects which address range comparator pairs are in use with ViewData include control.</p> <p><b>0b0</b></p> <p>The address range that address range comparator pair m defines, is not selected for ViewData include control.</p> <p><b>0b1</b></p> <p>The address range that address range comparator pair m defines, is selected for ViewData include control.</p> <p>If no single address comparators and no address range comparators are selected to be included, then all data transfers are included by default. The exclude control then indicates which data transfers are excluded.</p>	xxxx

Access

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, ext-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects an address range comparator that is programmed to be sensitive to a data value comparator, data transfers might be traced unexpectedly or might not be traced.

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

This register must be programmed when both of the following apply:

- Data tracing is enabled, that is, ext-TRCCONFIGR.DA==1 or ext-TRCCONFIGR.DV==1.
- One or more address comparators are implemented, that is, ext-TRCIDR4.NUMACPAIRS > 0b0000.

If software writes to this register and selects an address range comparator that is programmed to be sensitive to a data value comparator, data transfers might be traced unexpectedly or might not be traced.

Component	Offset	Range
ETM	0x0A8	None

This interface is accessible as follows:

RW

B.2.2.7.19 TRCSEQEVR<n>, Sequencer State Transition Control Register <n> , n = 0 - 2

Moves the sequencer state:

- Backwards, from state n+1 to state n when a programmed resource event occurs.
- Forwards, from state n to state n+1 when a programmed resource event occurs.

Configurations

External register TRCSEQEVR<n> bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.1 TRCSEQEVR<n>, Sequencer State Transition Control Register <n> , n = 0 - 2](#) on page 1261 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x100 + (4 \* n)

Access type

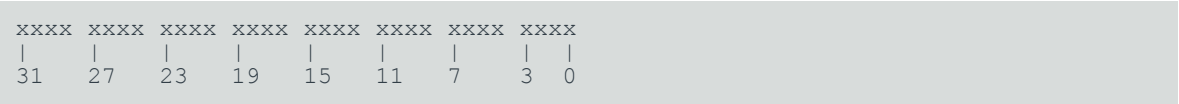
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-412: EXT\_TRCSEQEVR<n> bit assignments

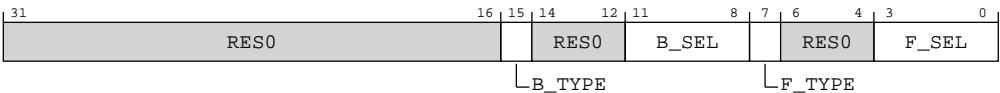


Table B-803: TRCSEQEVR<n> bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[15]	B_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Backward field. Defines whether the backward resource event is a single Resource Selector or a Resource Selector pair. When the resource event occurs then the sequencer state moves from state n+1 to state n. For example, if TRCSEQEVR2.B_SEL == 0x14 then when event 0x14 occurs, the sequencer moves from state 3 to state 2.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>B_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>B_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. B_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[14:12]	RES0	Reserved	RES0
[11:8]	B_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. B_TYPE controls whether B_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Backward field. Selects the single Resource Selector or Resource Selector pair.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx
[7]	F_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Forward field. Defines whether the forward resource event is a single Resource Selector or a Resource Selector pair. When the resource event occurs then the sequencer state moves from state n to state n+1. For example, if TRCSEQEVR1.F_SEL == 0x12 then when event 0x12 occurs, the sequencer moves from state 1 to state 2.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>F_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>F_SEL[2:0] selects the Resource Selector pair, from 0-15, that has a Boolean function that is applied to it whose output is used to activate the resource event. F_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[6:4]	RES0	Reserved	RES0
[3:0]	F_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. F_TYPE controls whether F_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Forward field. Selects the single Resource Selector or Resource Selector pair.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

Component	Offset	Range
ETM	0x100 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.20 TRCSEQRSTEV, Sequencer Reset Control Register

Moves the sequencer to state 0 when a programmed resource event occurs.

Configurations

External register TRCSEQRSTEV bits [31:0] are architecturally mapped to AArch64 System register A.2.8.20 TRCSEQRSTEV, Sequencer Reset Control Register on page 1302 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x118

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-413: EXT\_TRCSEQRSTEVSR bit assignments

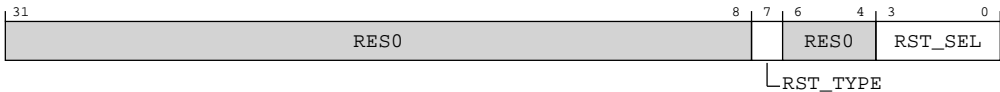


Table B-805: TRCSEQRSTEVSR bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7]	RST_TYPE	Chooses the type of Resource Selector.  <b>0b0</b> A single Resource Selector.  RST_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.  <b>0b1</b> A Boolean-combined pair of Resource Selectors.  RST_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. RST_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.	x
[6:4]	RES0	Reserved	RES0
[3:0]	RST_SEL	Defines the selected Resource Selector or pair of Resource Selectors. RST_TYPE controls whether RST_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.  If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b> , and the resource event might fire or might not fire.	xxxx

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

Component	Offset	Range
ETM	0x118	None

This interface is accessible as follows:

RW

B.2.2.7.21 TRCSEQSTR, Sequencer State Register

Use this to set, or read, the sequencer state.

Configurations

External register TRCSEQSTR bits [31:0] are architecturally mapped to AArch64 System register A.2.8.21 TRCSEQSTR, Sequencer State Register on page 1305 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x11C

Access type

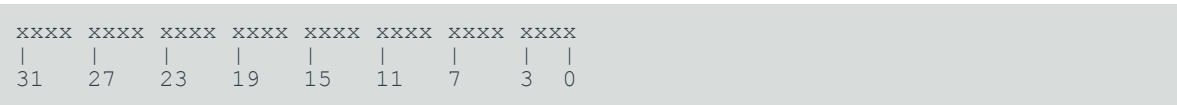
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-414: EXT\_TRCSEQSTR bit assignments

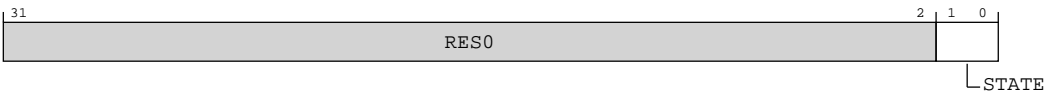


Table B-807: TRCSEQSTR bit descriptions

Bits	Name	Description	Reset
[31:2]	RES0	Reserved	RES0



Bits	Name	Description	Reset
[1:0]	STATE	Set or returns the state of the sequencer.  <b>0b00</b> State 0.  <b>0b01</b> State 1.  <b>0b10</b> State 2.  <b>0b11</b> State 3.	xx

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.SEQUENCER != 0b0000.

Component	Offset	Range
ETM	0x11C	None

This interface is accessible as follows:

RW

B.2.2.7.22 TRCEXTINSEL, External Input Select Register

Use this to set, or read, which external inputs are resources to the trace unit.

Configurations

External register TRCEXTINSEL bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.24 TRCEXTINSEL, External Input Select Register](#) on page 1313 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x120

Access type

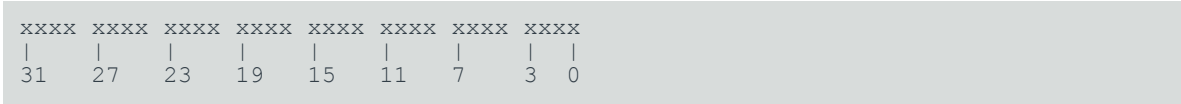
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-415: EXT\_TRCEXTINSELR bit assignments

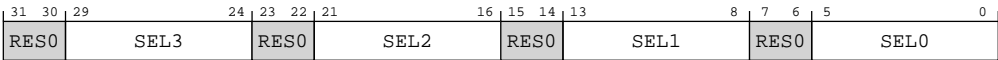


Table B-809: TRCEXTINSELR bit descriptions

Bits	Name	Description	Reset
[31:30]	RES0	Reserved	RES0
[29:24]	SEL3	Selects external input resource #3.	6 { x }
[23:22]	RES0	Reserved	RES0
[21:16]	SEL2	Selects external input resource #2.	6 { x }
[15:14]	RES0	Reserved	RES0
[13:8]	SEL1	Selects external input resource #1.	6 { x }
[7:6]	RES0	Reserved	RES0
[5:0]	SEL0	Selects external input resource #0.	6 { x }

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

Component	Offset	Range
ETM	0x120	None

This interface is accessible as follows:

RW

B.2.2.7.23 TRCCNTRLDVR<n>, Counter Reload Value Register <n> , n = 0 - 1

This sets or returns the reload count value for counter <n>.

Configurations

External register TRCCNTRLDVR<n> bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.2 TRCCNTRLDVR<n>, Counter Reload Value Register <n> , n = 0 - 1](#) on page 1264 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x140 + (4 \* n)

Access type

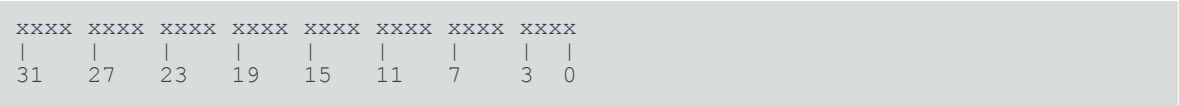
Read

R

Write

W

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-416: EXT\_TRCCNTRLDVR<n> bit assignments

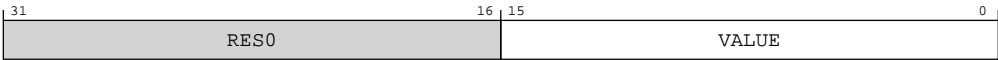


Table B-811: TRCCNTRLDVR<n> bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[15:0]	VALUE	Contains the reload value for counter <n>. When a reload event occurs for counter <n> then the trace unit copies the VALUE<n> field into counter <n>.	16 {x}

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

Component	Offset	Range
ETM	0x140 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.24 TRCCNTCTLR<n>, Counter Control Register <n> , n = 0 - 1

Controls the operation of counter <n>.

Configurations

External register TRCCNTCTLR<n> bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.3 TRCCNTCTLR<n>, Counter Control Register <n> , n = 0 - 1](#) on page 1266 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x150 + (4 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-417: EXT\_TRCCNTCTLR<n> bit assignments

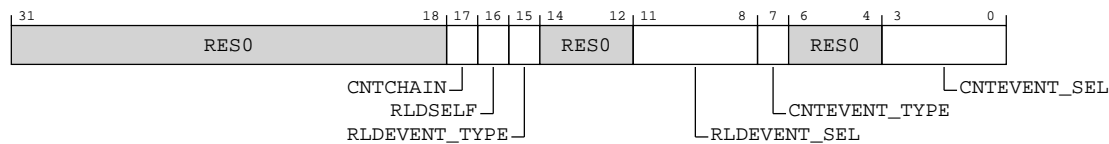


Table B-813: TRCCNTCTLR<n> bit descriptions

Bits	Name	Description	Reset
[31:18]	RES0	Reserved	RES0
[17]	CNTCHAIN	For TRCCNTCTLR1, this bit controls whether the counter decrements when a reload event occurs for counter <n-1>.  <b>0b0</b> The counter does not decrement when a reload event for counter <n-1> occurs.  <b>0b1</b> Counter <n> decrements when a reload event for counter <n-1> occurs. This concatenates counter <n> and counter <n-1>, to provide a larger count value.  CNTCHAIN is not implemented for TRCCNTCTLR0.	x
[16]	RLDSELF	Controls whether a reload event occurs for the counter, when the counter reaches zero.  <b>0b0</b> Normal mode.  The counter is in Normal mode.  <b>0b1</b> Self-reload mode.  The counter is in Self-reload mode.	x

Bits	Name	Description	Reset
[15]	RLDEVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Selects an event, that when it occurs causes a reload event for counter &lt;n&gt;.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>RLDEVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>RLDEVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. RLDEVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[14:12]	RES0	Reserved	RES0
[11:8]	RLDEVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. RLDEVENT_TYPE controls whether RLDEVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Selects an event, that when it occurs causes a reload event for counter &lt;n&gt;.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx
[7]	CNTEVENT_TYPE	<p>Chooses the type of Resource Selector.</p> <p>Selects an event, that when it occurs causes counter &lt;n&gt; to decrement.</p> <p><b>0b0</b></p> <p>A single Resource Selector.</p> <p>CNTEVENT_SEL[3:0] selects the single Resource Selector, from 0-15, used to activate the resource event.</p> <p><b>0b1</b></p> <p>A Boolean-combined pair of Resource Selectors.</p> <p>CNTEVENT_SEL[2:0] selects the Resource Selector pair, from 0-7, that has a Boolean function that is applied to it whose output is used to activate the resource event. CNTEVENT_SEL[3] is ignored by the Trace unit and behaves as if it was programmed to 0.</p>	x
[6:4]	RES0	Reserved	RES0
[3:0]	CNTEVENT_SEL	<p>Defines the selected Resource Selector or pair of Resource Selectors. CNTEVENT_TYPE controls whether CNTEVENT_SEL is the index of a single Resource Selector, or the index of a pair of Resource Selectors.</p> <p>Selects an event, that when it occurs causes counter &lt;n&gt; to decrement.</p> <p>If an unimplemented Resource Selector is selected using this field, the behavior of the resource event is <b>UNPREDICTABLE</b>, and the resource event might fire or might not fire.</p>	xxxx

## Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

Component	Offset	Range
ETM	0x150 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.25 TRCCNTVR<n>, Counter Value Register <n> , n = 0 - 1

This sets or returns the value of counter <n>.

Configurations

External register TRCCNTVR<n> bits [31:0] are architecturally mapped to AArch64 System register A.2.8.4 TRCCNTVR<n>, Counter Value Register <n> , n = 0 - 1 on page 1269 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x160 + (4 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-418: EXT\_TRCCNTVR<n> bit assignments

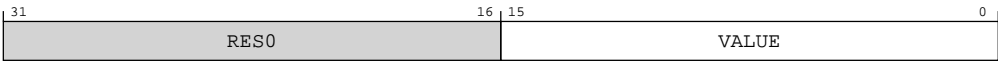


Table B-815: TRCCNTVR<n> bit descriptions

Bits	Name	Description	Reset
[31:16]	RES0	Reserved	RES0
[15:0]	VALUE	Contains the count value of counter.	16 { x }

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0010 and TRCRSCTLR<a>.COUNTERS[n] == 0b1.

Component	Offset	Range
ETM	0x160 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.26 TRCIDR8, ID Register 8

Returns the maximum speculation depth of the instruction trace element stream.

Configurations

External register TRCIDR8 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.7 TRCIDR8, ID Register 8](#) on page 1277 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x180

Access type

RO

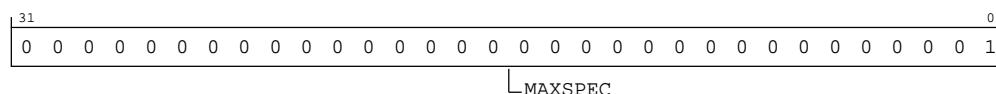
Reset value

0000 0000 0000 0000 0000 0000 0000 0001



## Bit descriptions

### Figure B-419: EXT\_TRCIDR8 bit assignments



### Table B-817: TRCIDR8 bit descriptions

Bits	Name	Description	Reset
[31:0]	MAXSPEC	<p>Indicates the maximum speculation depth of the instruction trace element stream. This is the maximum number of PO elements in the trace element stream that can be speculative at any time.</p> <p><b>0b00000000000000000000000000000001</b></p> <p>1 speculative PO element.</p>	0x00000001

## Accessibility

Component	Offset	Range
ETM	0x180	None

This interface is accessible as follows:

RO

#### B.2.2.7.27 TRCIDR9, ID Register 9

Returns the tracing capabilities of the trace unit.

## Configurations

External register TRCIDR9 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.11 TRCIDR9, ID Register 9](#) on page 1285 bits [31:0].

## Attributes

## Width

32

## Component

ETM

## Register offset

0x184

## Access type

RO

## Reset value

0000 0000 0000 0000 0000 0000 0010 0000

Bit descriptions

Figure B-420: EXT\_TRCIDR9 bit assignments

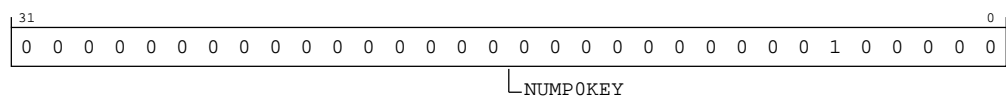


Table B-819: TRCIDR9 bit descriptions

Bits	Name	Description	Reset
[31:0]	NUMPOKEY	Indicates the number of PO right-hand keys.  0b0000000000000000000000000000100000 32 PO right-hand keys.	0x00000020

Accessibility

Component	Offset	Range
ETM	0x184	None

This interface is accessible as follows:

RO

B.2.2.7.28 TRCIDR10, ID Register 10

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR10 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.13 TRCIDR10, ID Register 10](#) on page 1289 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x188

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 1000

Bit descriptions

Figure B-421: EXT\_TRCIDR10 bit assignments

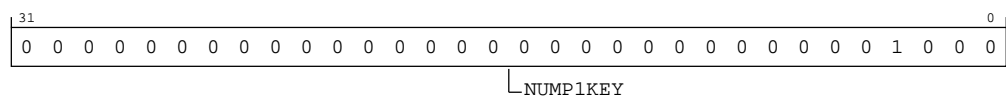


Table B-821: TRCIDR10 bit descriptions

Bits	Name	Description	Reset
[31:0]	NUMP1KEY	Indicates the number of P1 right-hand keys.  0b000000000000000000000000000001000 8 P1 right-hand keys.	0x00000008

Accessibility

Component	Offset	Range
ETM	0x188	None

This interface is accessible as follows:

RO

B.2.2.7.29 TRCIDR11, ID Register 11

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR11 bits [31:0] are architecturally mapped to AArch64 System register A.2.8.15 TRCIDR11, ID Register 11 on page 1292 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x18C

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-422: EXT\_TRCIDR11 bit assignments

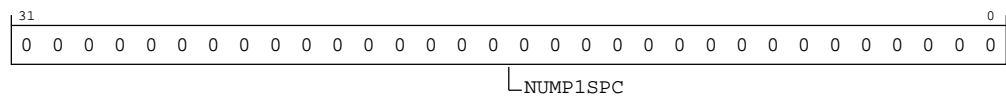


Table B-823: TRCIDR11 bit descriptions

Bits	Name	Description	Reset
[31:0]	NUMP1SPC	Indicates the number of special P1 right-hand keys.  0b00000000000000000000000000000000 No special P1 right-hand keys.	0x00000000

Accessibility

Component	Offset	Range
ETM	0x18C	None

This interface is accessible as follows:

RO

B.2.2.7.30 TRCIDR12, ID Register 12

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR12 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.17 TRCIDR12, ID Register 12](#) on page 1297 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x190

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0001

Bit descriptions

Figure B-423: EXT\_TRCIDR12 bit assignments

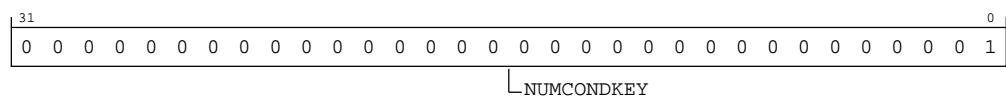


Table B-825: TRCIDR12 bit descriptions

Bits	Name	Description	Reset
[31:0]	NUMCONDKEY	Indicates the number of conditional instruction right-hand keys.  0b00000000000000000000000000000001 1 conditional instruction right-hand key.	0x00000001

Accessibility

Component	Offset	Range
ETM	0x190	None

This interface is accessible as follows:

RO

B.2.2.7.31 TRCIDR13, ID Register 13

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR13 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.18 TRCIDR13, ID Register 13](#) on page 1299 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x194

Access type

RO

Reset value

0000 0000 0000 0000 0000 0000 0000 0000

Bit descriptions

Figure B-424: EXT\_TRCIDR13 bit assignments

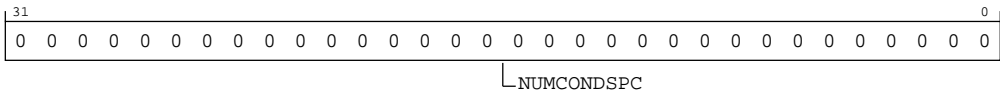


Table B-827: TRCIDR13 bit descriptions

Bits	Name	Description	Reset
[31:0]	NUMCONDSPC	Indicates the number of special conditional instruction right-hand keys.  0b00000000000000000000000000000000  No special conditional instruction right-hand keys.	0x00000000

Accessibility

Component	Offset	Range
ETM	0x194	None

This interface is accessible as follows:

RO

B.2.2.7.32 TRCIMSPECO, IMP DEF Register 0

TRCIMSPECO shows the presence of any **IMPLEMENTATION DEFINED** features, and provides an interface to enable the features that are provided.

Configurations

External register TRCIMSPECO bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.8 TRCIMSPECO, IMP DEF Register 0](#) on page 1279 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1C0


Access type

RO

Reset value



312723191511730



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-425: EXT\_TRCIMSPEC0 bit assignments

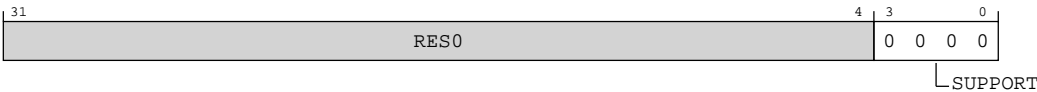


Table B-829: TRCIMSPEC0 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	SUPPORT	Indicates whether the implementation supports <b>IMPLEMENTATION DEFINED</b> features.  0b0000 No <b>IMPLEMENTATION DEFINED</b> features are supported.	0b0000

Accessibility

Component	Offset	Range
ETM	0x1C0	None

This interface is accessible as follows:

RW

B.2.2.7.33 TRCIDR0, ID Register 0

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.25 TRCIDR0, ID Register 0](#) on page 1315 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1E0

Access type

RO

Reset value

xx00	1000	xxxx	xx00	0x00	111x	1111	111x
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-426: EXT\_TRCIDR0 bit assignments

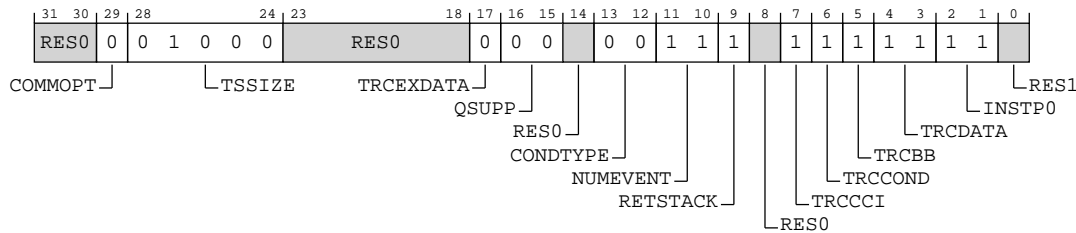


Table B-831: TRCIDR0 bit descriptions

Bits	Name	Description	Reset
[31:30]	RES0	Reserved	RES0
[29]	COMMOPT	Indicates how the commit field in Cycle count packets is interpreted.  <b>0b0</b>  Commit mode 0.  Cycle count packets includes the Commit element to which the Cycle Count element is attached.	0b0
[28:24]	TSSIZE	Indicates that the trace unit implements Global timestamping and the size of the timestamp value.  <b>0b01000</b>  Global timestamping implemented with a 64-bit timestamp value.	0b01000
[23:18]	RES0	Reserved	RES0
[17]	TRCEXDATA	Indicates if the trace unit implements tracing of data transfers for exceptions and exception returns.  <b>0b0</b>  Tracing of data transfers for exceptions and exception returns not implemented.	0b0



Bits	Name	Description	Reset
[16:15]	QSUPP	Indicates that the trace unit implements Q element support.  <b>0b00</b> Q element support is not implemented.	0b00
[14]	RES0	Reserved	RES0
[13:12]	CONDTYPE	Indicates how conditional instructions are traced.  <b>0b00</b> Conditional instructions are traced with an indication of whether they pass or fail their condition code check.	0b00
[11:10]	NUMEVENT	Indicates the number of trace events implemented.  <b>0b11</b> The trace unit supports 4 trace events.	0b11
[9]	RETSTACK	Indicates if the trace unit supports the return stack.  <b>0b1</b> Return stack implemented.	0b1
[8]	RES0	Reserved	RES0
[7]	TRCCCI	Indicates if the trace unit implements cycle counting.  <b>0b1</b> Cycle counting implemented.	0b1
[6]	TRCCOND	Indicates if the trace unit implements conditional instruction tracing.  <b>0b1</b> Conditional instruction tracing implemented.	0b1
[5]	TRCBB	Indicates if the trace unit implements branch broadcasting.  <b>0b1</b> Branch broadcasting implemented.	0b1
[4:3]	TRCDATA	Indicates if the trace unit implements data tracing.  <b>0b11</b> Data tracing implemented.	0b11
[2:1]	INSTP0	Indicates if load and store instructions are P0 instructions.  <b>0b11</b> Load and store instructions are P0 instructions.	0b11
[0]	RES1	Reserved	RES1

## Accessibility

Component	Offset	Range
ETM	0x1E0	None

This interface is accessible as follows:

RO

B.2.2.7.34 TRCIDR1, ID Register 1

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.28 TRCIDR1, ID Register 1](#) on page 1324 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1E4

Access type

RO

Reset value

0100	0001	xxxx	xxxx	xxxx	0100	0101	0111
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-427: EXT\_TRCIDR1 bit assignments

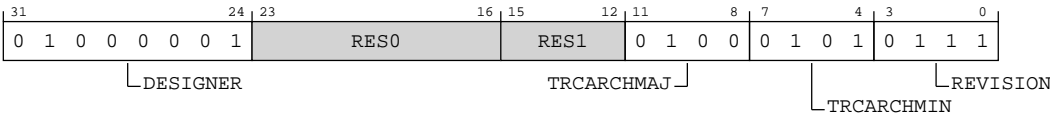


Table B-833: TRCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:24]	DESIGNER	Indicates which company designed the trace unit.  <b>0b01000001</b> Arm Limited.	0x41
[23:16]	RES0	Reserved	RES0
[15:12]	RES1	Reserved	RES1

Bits	Name	Description	Reset
[11:8]	TRCARCHMAJ	Major architecture version.  <b>0b0100</b> ETMv4.	0b0100
[7:4]	TRCARCHMIN	Minor architecture version.  <b>0b0101</b> ETMv4.5.  All other values are reserved.	0b0101
[3:0]	REVISION	Implementation revision.  <b>0b0111</b> Revision 7.	0b0111

Accessibility

Component	Offset	Range
ETM	0x1E4	None

This interface is accessible as follows:

RO

B.2.2.7.35 TRCIDR2, ID Register 2

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR2 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.30 TRCIDR2, ID Register 2](#) on page 1328 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1E8

Access type

RO

Reset value

1100 0000 1000 0100 0001 0000 1000 1000

Bit descriptions

Figure B-428: EXT\_TRCIDR2 bit assignments

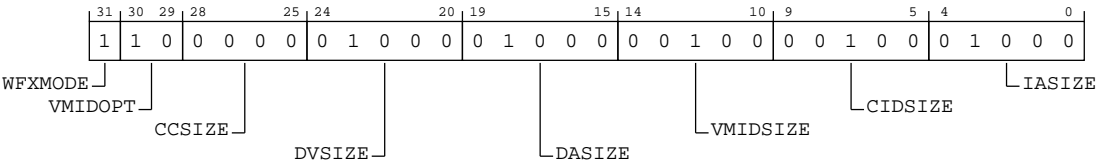


Table B-835: TRCIDR2 bit descriptions

Bits	Name	Description	Reset
[31]	WFXMODE	Indicates whether WFI and WFE instructions are classified as PO instructions: <b>0b1</b> WFI and WFE instructions are classified as PO instructions.	0b1
[30:29]	VMIDOPT	Indicates the options for Virtual context identifier selection. <b>0b10</b> Virtual context identifier selection not supported. ext-TRCCONFIGR.VMIDOPT is <b>RES1</b> .	0b10
[28:25]	CCSIZE	Indicates the size of the cycle counter. <b>0b0000</b> The cycle counter is 12 bits in length.	0b0000
[24:20]	DVSIZE	Indicates the data value size in bytes. <b>0b01000</b> Data value tracing has a maximum of 64-bit data values.	0b01000
[19:15]	DASIZE	Indicates the data address size in bytes. <b>0b01000</b> Data address tracing has a maximum of 64-bit data addresses.	0b01000
[14:10]	VMIDSIZE	Indicates the trace unit Virtual context identifier size. <b>0b00100</b> 32-bit Virtual context identifier size.	0b00100
[9:5]	CIDSIZE	Indicates the Context identifier size. <b>0b00100</b> 32-bit Context identifier size.	0b00100
[4:0]	IASIZE	Virtual instruction address size. <b>0b01000</b> Maximum of 64-bit instruction address size.	0b01000

Accessibility

Component	Offset	Range
ETM	0x1E8	None

This interface is accessible as follows:

RO

B.2.2.7.36 TRCIDR3, ID Register 3

Returns the base architecture of the trace unit.

Configurations

External register TRCIDR3 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.32 TRCIDR3, ID Register 3](#) on page 1333 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1EC

Access type

RO

Reset value

x000	1101	x000	0111	xx00	0000	0000	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-429: EXT\_TRCIDR3 bit assignments

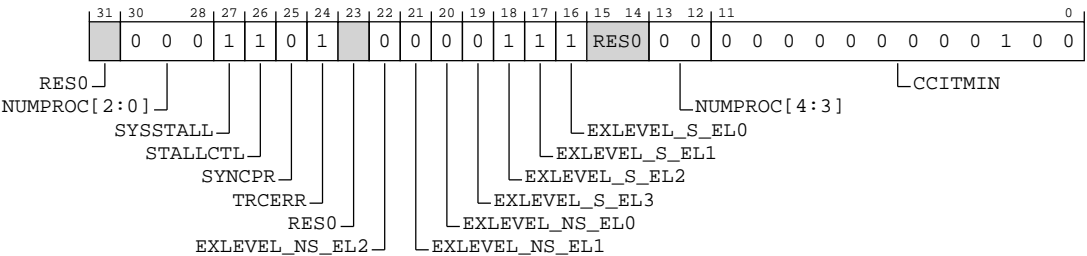


Table B-837: TRCIDR3 bit descriptions

Bits	Name	Description	Reset
[31]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[27]	SYSSTALL	Indicates if stalling of the PE is permitted. <b>0b1</b> Stalling of the PE is permitted.	0b1
[26]	STALLCTL	Indicates if trace unit implements stalling of the PE. <b>0b1</b> Stalling of the PE is implemented.	0b1
[25]	SYNCPR	Indicates if an implementation has a fixed synchronization period. <b>0b0</b> ext-TRCSYNCPR is read-write so software can change the synchronization period.	0b0
[24]	TRCERR	Indicates forced tracing of System Error exceptions is implemented. <b>0b1</b> Forced tracing of System Error exceptions is implemented.	0b1
[23]	<b>RES0</b>	Reserved	<b>RES0</b>
[22]	EXLEVEL_NS_EL2	Indicates if Non-secure EL2 implemented. <b>0b0</b> Non-secure EL2 is not implemented.	0b0
[21]	EXLEVEL_NS_EL1	Indicates if Non-secure EL1 implemented. <b>0b0</b> Non-secure EL1 is not implemented.	0b0
[20]	EXLEVEL_NS_ELO	Indicates if Non-secure ELO implemented. <b>0b0</b> Non-secure ELO is not implemented.	0b0
[19]	EXLEVEL_S_EL3	Indicates if Secure EL3 implemented. <b>0b0</b> Secure EL3 is not implemented.	0b0
[18]	EXLEVEL_S_EL2	Indicates if Secure EL2 implemented. <b>0b1</b> Secure EL2 is implemented.	0b1
[17]	EXLEVEL_S_EL1	Indicates if Secure EL1 implemented. <b>0b1</b> Secure EL1 is implemented.	0b1
[16]	EXLEVEL_S_ELO	Indicates if Secure ELO implemented. <b>0b1</b> Secure ELO is implemented.	0b1
[15:14]	<b>RES0</b>	Reserved	<b>RES0</b>
[13:12, 30:28]	NUMPROC	Indicates the number of PEs available for tracing. <b>0b00000</b> The trace unit can trace one PE.  This field reads as 0b00000.	0b00000

Bits	Name	Description	Reset
[11:0]	CCITMIN	Indicates the minimum value that can be programmed in ext-TRCCCCTLR.THRESHOLD. <b>0b0000000000100</b> Minimum allowed threshold value is 4.	0x004

Accessibility

Component	Offset	Range
ETM	0x1EC	None

This interface is accessible as follows:

RO

B.2.2.7.37 TRCIDR4, ID Register 4

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR4 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.34 TRCIDR4, ID Register 4](#) on page 1338 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1F0

Access type

RO

Reset value

0001	0001	0010	0111	0000	xxx1	0010	0100
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-430: EXT\_TRCIDR4 bit assignments

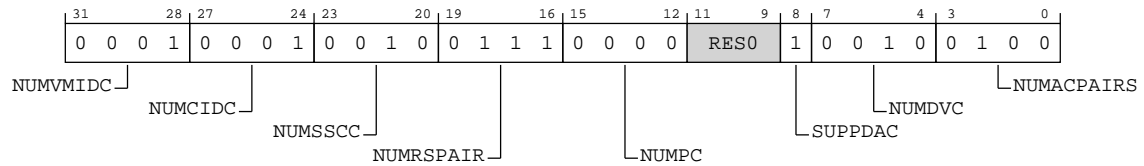


Table B-839: TRCIDR4 bit descriptions

Bits	Name	Description	Reset
[31:28]	NUMVMIDC	Indicates the number of Virtual Context Identifier Comparators that are available for tracing. <b>0b0001</b> The implementation has one Virtual Context Identifier Comparator.	0b0001
[27:24]	NUMCIDC	Indicates the number of Context Identifier Comparators that are available for tracing. <b>0b0001</b> The implementation has one Context Identifier Comparator.	0b0001
[23:20]	NUMSSCC	Indicates the number of Single-shot Comparator Controls that are available for tracing. <b>0b0010</b> The implementation has two Single-shot Comparator Controls.	0b0010
[19:16]	NUMRSPAIR	Indicates the number of resource selector pairs that are available for tracing. <b>0b0111</b> The implementation has eight resource selector pairs.	0b0111
[15:12]	NUMPC	Indicates the number of PE Comparator Inputs that are available for tracing. <b>0b0000</b> No PE Comparator Inputs are available.	0b0000
[11:9]	RES0	Reserved	RES0
[8]	SUPPDAC	Indicates whether data address comparisons are implemented. <b>0b1</b> Data address comparisons implemented.	0b1
[7:4]	NUMDVC	Indicates the number of data value comparators. <b>0b0010</b> Two data value comparators implemented.	0b0010
[3:0]	NUMACPAIRS	Indicates the number of address comparator pairs that are available for tracing. <b>0b0100</b> The implementation has four address comparator pairs.	0b0100

## Accessibility

Component	Offset	Range
ETM	0x1F0	None

This interface is accessible as follows:



RO

B.2.2.7.38 TRCIDR5, ID Register 5

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR5 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.36 TRCIDR5, ID Register 5](#) on page 1343 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1F4

Access type

RO

Reset value

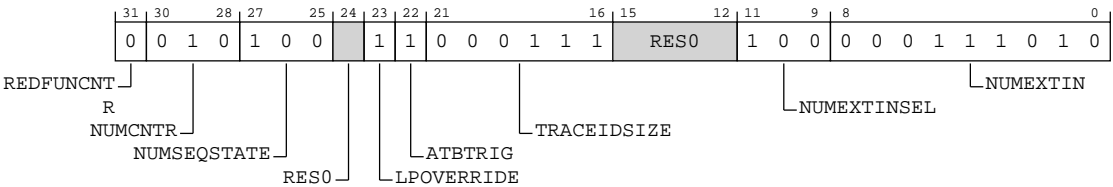
0010	100x	1100	0111	xxxx	1000	0011	1010
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-431: EXT\_TRCIDR5 bit assignments



**Table B-841: TRCIDR5 bit descriptions**

Bits	Name	Description	Reset
[31]	REDFUNCNTR	Indicates if the reduced function counter is implemented. <b>0b0</b> The reduced function counter is not supported.	0b0
[30:28]	NUMCNTR	Indicates the number of counters that are available for tracing. <b>0b010</b> Two counters implemented.	0b010
[27:25]	NUMSEQSTATE	Indicates if the sequencer is implemented and the number of sequencer states that are implemented. <b>0b100</b> Four sequencer states are implemented.	0b100
[24]	RES0	Reserved	RES0
[23]	LPOVERRIDE	Indicates support for Low-power Override Mode. <b>0b1</b> The trace unit support Low-power Override Mode.	0b1
[22]	ATBTRIG	Indicates if the implementation can support ATB triggers. <b>0b1</b> The implementation supports ATB triggers.	0b1
[21:16]	TRACEIDSIZE	Indicates the trace ID width. <b>0b000111</b> The implementation supports a 7-bit trace ID.	0b000111
[15:12]	RES0	Reserved	RES0
[11:9]	NUMEXTINSEL	Indicates how many external input selector resources are implemented. <b>0b100</b> 4 external input selector resources are available.	0b100
[8:0]	NUMEXTIN	Indicates how many external inputs are implemented. <b>0b000111010</b> The implementation has 58 external inputs.	0b000111010

### Accessibility

Component	Offset	Range
ETM	0x1F4	None

This interface is accessible as follows:

RO

B.2.2.7.39 TRCIDR6, ID Register 6

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR6 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.38 TRCIDR6, ID Register 6](#) on page 1347 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x1F8

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-432: EXT\_TRCIDR6 bit assignments

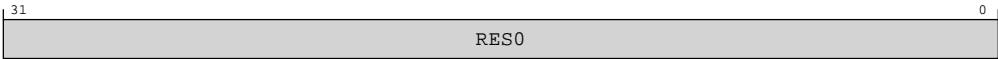


Table B-843: TRCIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0x1F8	None

This interface is accessible as follows:

RO

B.2.2.7.40 TRCIDR7, ID Register 7

Returns the tracing capabilities of the trace unit.

Configurations

External register TRCIDR7 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.40 TRCIDR7, ID Register 7](#) on page 1351 bits [31:0].

Attributes

Width

32

Component

ETM

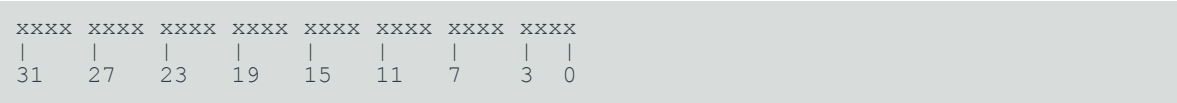
Register offset

0x1FC

Access type

RO

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-433: EXT\_TRCIDR7 bit assignments

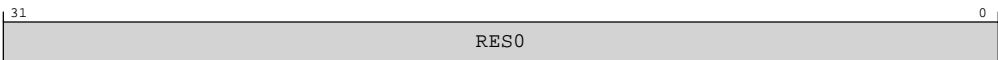


Table B-845: TRCIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0x1FC	None

This interface is accessible as follows:

RO

B.2.2.7.41 TRCRSCTLR<n>, Resource Selection Control Register <n> , n = 2 - 15

Controls the selection of the resources in the trace unit.

Configurations

Resource selector 0 always returns FALSE.

Resource selector 1 always returns TRUE.

Resource selectors are implemented in pairs. Each odd numbered resource selector is part of a pair with the even numbered resource selector that is numbered as one less than it. For example, resource selectors 2 and 3 form a pair.

External register TRCRSCTLR<n> bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.45 TRCRSCTLR<n>, Resource Selection Control Register <n> , n = 2 - 15](#) on page 1361 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x200 + (4 \* n)

Access type

Read

R

Write

W

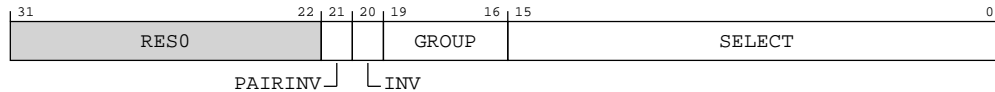
Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-434: EXT\_TRCRSCTLR<n> bit assignments****Table B-847: TRCRSCTLR<n> bit descriptions**

Bits	Name	Description	Reset
[31:22]	RES0	Reserved	RES0
[21]	PAIRINV	For TRCRSCTLR<n>, where n is even, controls whether the combined result from a resource selector pair is inverted.  <b>0b0</b> Do not invert the combined output of the 2 resource selectors.  <b>0b1</b> Invert the combined output of the 2 resource selectors.	x
[20]	INV	Controls whether the resource, that GROUP and SELECT selects, is inverted.  <b>0b0</b> Do not invert the output of this selector.  <b>0b1</b> Invert the output of this selector.  If: <ul style="list-style-type: none"> <li>A is the register TRCRSCTLR&lt;m&gt; where m is even.</li> <li>B is the register TRCRSCTLR&lt;m+1&gt;.</li> </ul> Then the combined output of the 2 resource selectors A and B depends on the value of (A.PAIRINV, A.INV, B.INV) as follows: <ul style="list-style-type: none"> <li>0b000 -&gt; A and B.</li> <li>0b001 -&gt; RESERVED.</li> <li>0b010 -&gt; not(A) and B.</li> <li>0b011 -&gt; not(A) and not(B).</li> <li>0b100 -&gt; not(A) or not(B).</li> <li>0b101 -&gt; not(A) or B.</li> <li>0b110 -&gt; RESERVED.</li> <li>0b111 -&gt; A or B.</li> </ul>	x

Bits	Name	Description	Reset
[19:16]	GROUP	<p>Selects a group of resources.</p> <p><b>0b0000</b> External input selectors.</p> <p><b>0b0001</b> PE Comparator Inputs.</p> <p><b>0b0010</b> Counters and Sequencer.</p> <p><b>0b0011</b> Single-shot Comparator Controls.</p> <p><b>0b0100</b> Single Address Comparators.</p> <p><b>0b0101</b> Address Range Comparators.</p> <p><b>0b0110</b> Context Identifier Comparators.</p> <p><b>0b0111</b> Virtual Context Identifier Comparators.</p> <p>All other values are reserved.</p>	xxxx
[15:0]	SELECT	<p><b>SELECT encoding for External input selectors</b></p> <p><b>15:4</b> Reserved, <b>RES0</b>.</p> <p><b>EXTIN&lt;m&gt;, bit[m], for m = 3 to 0</b> Selects one or more External inputs.</p> <p><b>0b0</b> Ignore EXTIN m.</p> <p><b>0b1</b> Select EXTIN m.</p>	16{x}
[15:0 continued]	SELECT	<p><b>SELECT encoding for PE Comparator Inputs</b></p> <p><b>15:0</b> Reserved, <b>RES0</b>.</p>	16{x}
[15:0 continued]	SELECT	<p><b>SELECT encoding for Counters and Sequencer</b></p> <p><b>15:8</b> Reserved, <b>RES0</b>.</p>	16{x}

Bits	Name	Description	Reset
[15:0 continued]	SELECT	<b>SEQUENCER&lt;m&gt;, bit[m], for m = 7 to 4</b> Sequencer states. <b>0b0</b> Ignore Sequencer state m. <b>0b1</b> Select Sequencer state m.  <b>3:2</b> Reserved, RES0.  <b>COUNTERS&lt;m&gt;, bit[m], for m = 1 to 0</b> Counters resources at zero. <b>0b0</b> Ignore Counter m. <b>0b1</b> Select Counter m is zero.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Single-shot Comparator Controls</b> <b>15:2</b> Reserved, RES0.  <b>SINGLE_SHOT&lt;m&gt;, bit[m], for m = 1 to 0</b> Selects one or more Single-shot Comparator Controls. <b>0b0</b> Ignore Single-shot Comparator Control m. <b>0b1</b> Select Single-shot Comparator Control m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Single Address Comparators</b> <b>15:8</b> Reserved, RES0.  <b>SAC&lt;m&gt;, bit[m], for m = 7 to 0</b> Selects one or more Single Address Comparators. <b>0b0</b> Ignore Single Address Comparator m. <b>0b1</b> Select Single Address Comparator m.	16 {x}



Bits	Name	Description	Reset
[15:0 continued]	SELECT	<b>SELECT encoding for Address Range Comparators</b>  <b>15:4</b> Reserved, RES0.  <b>ARC&lt;m&gt;, bit[m], for m = 3 to 0</b> Selects one or more Address Range Comparators.  <b>0b0</b> Ignore Address Range Comparator m.  <b>0b1</b> Select Address Range Comparator m.	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Context Identifier Comparators</b>  <b>15:1</b> Reserved, RES0.  <b>CID&lt;m&gt;, bit[m], for m = 0</b> Selects one or more Context Identifier Comparators.  <b>0b0</b> Ignore Context Identifier Comparator m.  <b>0b1</b> Select Context Identifier Comparator m	16 {x}
[15:0 continued]	SELECT	<b>SELECT encoding for Virtual Context Identifier Comparators</b>  <b>15:1</b> Reserved, RES0.	16 {x}
[15:0 continued]	SELECT	<b>VMID&lt;m&gt;, bit[m], for m = 0</b> Selects one or more Virtual Context Identifier Comparators.  <b>0b0</b> Ignore Virtual Context Identifier Comparator m.  <b>0b1</b> Select Virtual Context Identifier Comparator m.	16 {x}

## Access

Must be programmed if any of the following are true:

- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.RLDEVENT.SEL == n.
- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.RLDEVENT.SEL == n/2.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.CNTEVENT.SEL == n.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.CNTEVENT.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT0.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT0.SEL == n.
- ext-TRCEVENTCTLOR.EVENT0.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT0.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT1.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT1.SEL == n.

- ext-TRCEVENTCTLOR.EVENT1.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT1.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT2.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT2.SEL == n.
- ext-TRCEVENTCTLOR.EVENT2.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT2.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT3.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT3.SEL == n.
- ext-TRCEVENTCTLOR.EVENT3.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT3.SEL == n/2.
- TRCSEQEVR<a>.B.TYPE == 0b0 and TRCSEQEVR<a>.B.SEL = n.
- TRCSEQEVR<a>.B.TYPE == 0b1 and TRCSEQEVR<a>.B.SEL = n/2.
- TRCSEQEVR<a>.F.TYPE == 0b0 and TRCSEQEVR<a>.F.SEL = n.
- TRCSEQEVR<a>.F.TYPE == 0b1 and TRCSEQEVR<a>.F.SEL = n/2.
- ext-TRCSEQRSTEV.RST.TYPE == 0b0 and ext-TRCSEQRSTEV.RST.SEL == n.
- ext-TRCSEQRSTEV.RST.TYPE == 0b1 and ext-TRCSEQRSTEV.RST.SEL == n/2.
- ext-TRCTSCTLR.EVENT.TYPE == 0b0 and ext-TRCTSCTLR.EVENT.SEL == n.
- ext-TRCTSCTLR.EVENT.TYPE == 0b1 and ext-TRCTSCTLR.EVENT.SEL == n/2.
- ext-TRCVICTLR.EVENT.TYPE == 0b0 and ext-TRCVICTLR.EVENT.SEL == n.
- ext-TRCVICTLR.EVENT.TYPE == 0b1 and ext-TRCVICTLR.EVENT.SEL == n/2.

## Accessibility

Must be programmed if any of the following are true:

- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.RLDEVENT.SEL == n.
- TRCCNTCTLR<a>.RLDEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.RLDEVENT.SEL == n/2.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b0 and TRCCNTCTLR<a>.CNTEVENT.SEL == n.
- TRCCNTCTLR<a>.CNTEVENT.TYPE == 0b1 and TRCCNTCTLR<a>.CNTEVENT.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT0.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT0.SEL == n.
- ext-TRCEVENTCTLOR.EVENT0.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT0.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT1.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT1.SEL == n.
- ext-TRCEVENTCTLOR.EVENT1.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT1.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT2.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT2.SEL == n.
- ext-TRCEVENTCTLOR.EVENT2.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT2.SEL == n/2.
- ext-TRCEVENTCTLOR.EVENT3.TYPE == 0b0 and ext-TRCEVENTCTLOR.EVENT3.SEL == n.
- ext-TRCEVENTCTLOR.EVENT3.TYPE == 0b1 and ext-TRCEVENTCTLOR.EVENT3.SEL == n/2.

- TRCSEQEVR<a>.B.TYPE == 0b0 and TRCSEQEVR<a>.B.SEL = n.
- TRCSEQEVR<a>.B.TYPE == 0b1 and TRCSEQEVR<a>.B.SEL = n/2.
- TRCSEQEVR<a>.F.TYPE == 0b0 and TRCSEQEVR<a>.F.SEL = n.
- TRCSEQEVR<a>.F.TYPE == 0b1 and TRCSEQEVR<a>.F.SEL = n/2.
- ext-TRCSEQRSTEVR.RST.TYPE == 0b0 and ext-TRCSEQRSTEVR.RST.SEL == n.
- ext-TRCSEQRSTEVR.RST.TYPE == 0b1 and ext-TRCSEQRSTEVR.RST.SEL == n/2.
- ext-TRCTSCTLR.EVENT.TYPE == 0b0 and ext-TRCTSCTLR.EVENT.SEL == n.
- ext-TRCTSCTLR.EVENT.TYPE == 0b1 and ext-TRCTSCTLR.EVENT.SEL == n/2.
- ext-TRCVICTLR.EVENT.TYPE == 0b0 and ext-TRCVICTLR.EVENT.SEL == n.
- ext-TRCVICTLR.EVENT.TYPE == 0b1 and ext-TRCVICTLR.EVENT.SEL == n/2.

Component	Offset	Range
ETM	0x200 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.42 TRCSSCCR<n>, Single-shot Comparator Control Register <n> , n = 0 - 1

Controls the corresponding Single-shot Comparator Control resource.

Configurations

External register TRCSSCCR<n> bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.41 TRCSSCCR<n>, Single-shot Comparator Control Register <n> , n = 0 - 1](#) on page 1352 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x280 + (4 \* n)

Access type

Read

R

Write

W

## Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

Figure B-435: EXT\_TRCSSCCR<n> bit assignments

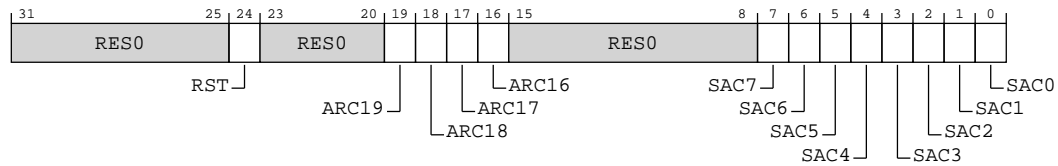


Table B-849: TRCSSCCR<n> bit descriptions

Bits	Name	Description	Reset
[31:25]	RES0	Reserved	RES0
[24]	RST	Selects the Single-shot Comparator Control mode. <b>0b0</b> The Single-shot Comparator Control is in single-shot mode. <b>0b1</b> The Single-shot Comparator Control is in multi-shot mode.	x
[23:20]	RES0	Reserved	RES0
[19:16]	ARC<m>, bit[m], where m = 19 to 16	Selects one or more Address Range Comparators for Single-shot control. <b>0b0</b> The Address Range Comparator m, is not selected for Single-shot control. <b>0b1</b> The Address Range Comparator m, is selected for Single-shot control.	xxxx
[15:8]	RES0	Reserved	RES0
[7:0]	SAC<m>, bit[m], where m = 7 to 0	Selects one or more Single Address Comparators for Single-shot control. <b>0b0</b> The Single Address Comparator m, is not selected for Single-shot control. <b>0b1</b> The Single Address Comparator m, is selected for Single-shot control.	8 {x}

## Accessibility

Must be programmed if any TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

Component	Offset	Range
ETM	0x280 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.43 TRCSSCSR<n>, Single-shot Comparator Control Status Register <n> , n = 0 - 1

Returns the status of the corresponding Single-shot Comparator Control.

Configurations

External register TRCSSCSR<n> bits [31:0] are architecturally mapped to AArch64 System register A.2.8.42 TRCSSCSR<n>, Single-shot Comparator Control Status Register <n> , n = 0 - 1 on page 1355 bits [31:0].

Attributes

Width

32

Component

ETM

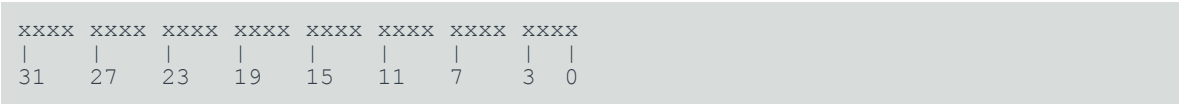
Register offset

0x2A0 + (4 \* n)

Access type

RO

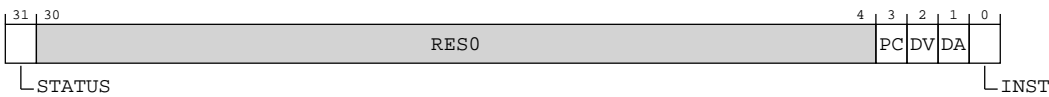
Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-436: EXT\_TRCSSCSR<n> bit assignments



**Table B-851: TRCSSCSR<n> bit descriptions**

Bits	Name	Description	Reset
[31]	STATUS	<p>Single-shot Comparator Control status. Indicates if any of the comparators selected by this Single-shot Comparator control have matched. The selected comparators are defined by ext-TRCSSCCR&lt;n&gt;.ARC and ext-TRCSSCCR&lt;n&gt;.SAC.</p> <p><b>0b0</b></p> <p>No match has occurred. When the first match occurs, this field takes a value of 0b1. It remains at 0b1 until explicitly modified by a write to this register.</p> <p><b>0b1</b></p> <p>One or more matches has occurred. If ext-TRCSSCCR&lt;n&gt;.RST == 0b0 then:</p> <ul style="list-style-type: none"> <li>There is only one match and no more matches are possible.</li> <li>Software must reset this bit to 0b0 to re-enable the Single-shot Comparator Control.</li> </ul> <p>The reset value is <b>UNKNOWN</b>. STATUS must be written to set an initial state when programming the trace unit, if the single-shot comparator is to be used.</p>	x
[30:4]	RES0	Reserved	RES0
[3]	PC	<p>PE Comparator Input support.</p> <p><b>0b0</b></p> <p>This Single-shot Comparator Control does not support PE Comparator Inputs.</p> <p>Access to this field is: RO</p>	x
[2]	DV	<p><b>When n == 0</b></p> <p>Data value comparator support.</p> <p><b>0</b></p> <p>This Single-shot Comparator Control does not support data value comparisons. TRCSSCSR0 has this value.</p> <p><b>When n == 1</b></p> <p>Data value comparator support.</p> <p><b>1</b></p> <p>This Single-shot Comparator Control supports data value comparisons. TRCSSCSR1 has this value.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x
[1]	DA	<p><b>When n == 0</b></p> <p>Data address comparator support.</p> <p><b>0</b></p> <p>This Single-shot Comparator Control does not support data address comparisons. TRCSSCSR0 has this value.</p> <p><b>When n == 1</b></p> <p>Data address comparator support.</p> <p><b>1</b></p> <p>This Single-shot Comparator Control supports data address comparisons. TRCSSCSR1 has this value.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x

Bits	Name	Description	Reset
[0]	INST	<p><b>When n == 0</b></p> <p>Instruction address comparator support.</p> <p><b>1</b></p> <p>This Single-shot Comparator Control supports instruction address comparisons. TRCSSCSR0 has this value.</p> <p><b>When n == 1</b></p> <p>Instruction address comparator support.</p> <p><b>0</b></p> <p>This Single-shot Comparator Control does not support instruction address comparisons. TRCSSCSR1 has this value.</p> <p><b>Otherwise</b></p> <p>RES0</p>	x

Accessibility

Must be programmed if TRCRSCTLR<a>.GROUP == 0b0011 and TRCRSCTLR<a>.SINGLE\_SHOT[n] == 0b1.

Component	Offset	Range
ETM	0x2A0 + (4 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.44 TRCOSLAR, Trace OS Lock Access Register

Controls whether the Trace OS Lock is locked.

Configurations

External register TRCOSLAR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.43 TRCOSLAR, Trace OS Lock Access Register](#) on page 1358 bits [31:0].

Attributes

Width

32

Component

ETM

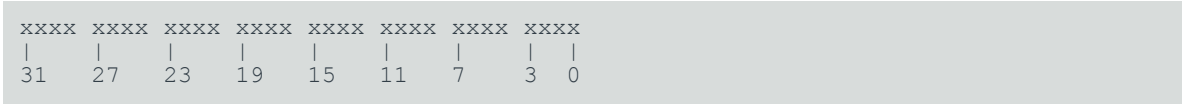
Register offset

0x300

Access type

RESERVEDW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-437: EXT\_TRCOSLAR bit assignments

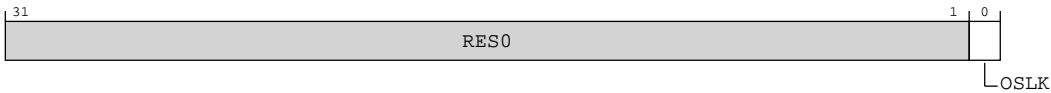


Table B-853: TRCOSLAR bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	OSLK	OS Lock control bit.  <b>0b0</b> Unlocks the OS Lock.  <b>0b1</b> Locks the OS Lock. This setting disables the trace unit.	x

Accessibility

Component	Offset	Range
ETM	0x300	None

This interface is accessible as follows:

WO

B.2.2.7.45 TRCOSLSR, Trace OS Lock Status Register

Returns the status of the Trace OS Lock.

Configurations

External register TRCOSLSR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.44 TRCOSLSR, Trace OS Lock Status Register](#) on page 1359 bits [31:0].



Attributes

Width

32

Component

ETM

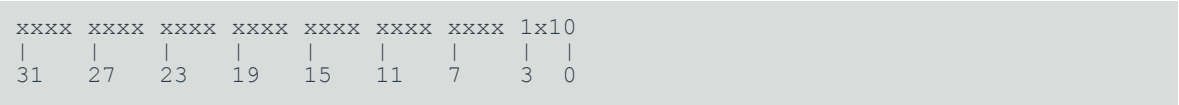
Register offset

0x304

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-438: EXT\_TRCOSLSR bit assignments

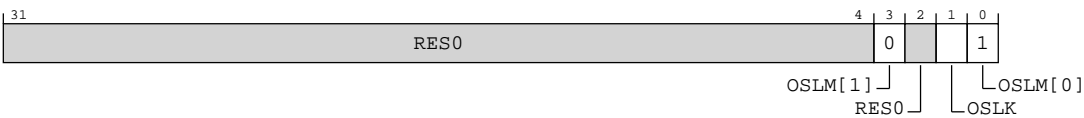


Table B-855: TRCOSLSR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3, 0]	OSLM	OS Lock model.  <b>0b10</b> Trace OS Lock is implemented.  Access to this field is: RO	0b10
[2]	RES0	Reserved	RES0
[1]	OSLK	OS Lock status.  <b>0b0</b> The OS Lock is unlocked.  <b>0b1</b> The OS Lock is locked.	0b1

Accessibility

Component	Offset	Range
ETM	0x304	None

This interface is accessible as follows:

RO

B.2.2.7.46 TRCPDCR, PowerDown Control Register

Legacy power control register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

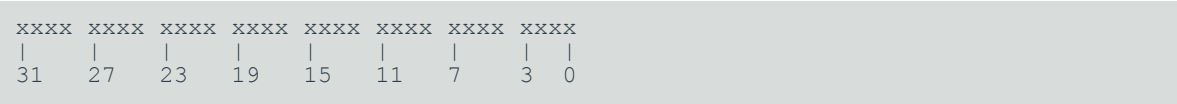
Register offset

0x310

Access type

RW

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-439: EXT\_TRCPDCR bit assignments

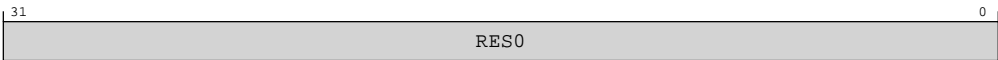


Table B-857: TRCPDCR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0x310	None

This interface is accessible as follows:

RW

B.2.2.7.47 TRCPDSR, PowerDown Status Register

Legacy power status register.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0x314

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xx11
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-440: EXT\_TRCPDSR bit assignments

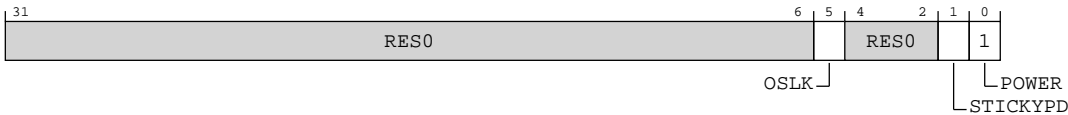


Table B-859: TRCPDSR bit descriptions

Bits	Name	Description	Reset
[31:6]	RES0	Reserved	RES0
[5]	OSLK	OS Lock Status.  0b0 The OS Lock is unlocked.  0b1 The OS Lock is locked.	x
[4:2]	RES0	Reserved	RES0
[1]	STICKYPD	Sticky powerdown status. Indicates whether the trace register state is valid.  0b0 The state of ext-TRCOSLSR and the trace registers are valid.  0b1 The state of ext-TRCOSLSR and the trace registers might not be valid.  This field is set to 1 if the power to the trace unit core power domain is removed and the trace unit register state is not valid.  The STICKYPD field is read-sensitive. On a read of the TRCPDSR, this field is cleared to 0 after the register has been read.	0b1
[0]	POWER	Power Status.  0b1 The trace unit core power domain is powered. Trace unit registers are accessible.	0b1

Accessibility

Component	Offset	Range
ETM	0x314	None

This interface is accessible as follows:

RO

B.2.2.7.48 TRCACVR<n>, Address Comparator Value Register <n> , n = 0 - 7

Contains the address value.

Configurations

External register TRCACVR<n> bits [63:0] are architecturally mapped to AArch64 System register A.2.8.48 TRCACVR<n>, Address Comparator Value Register <n> , n = 0 - 7 on page 1372 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

0x400 + (8 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0

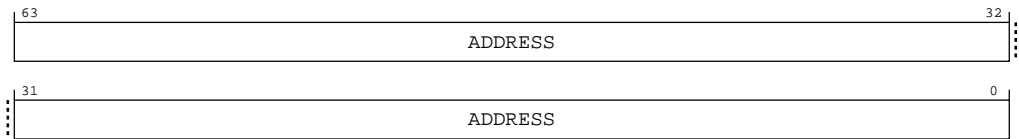


Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-441: EXT\_TRCACVR<n> bit assignments



**Table B-861: TRCACVR<n> bit descriptions**

Bits	Name	Description	Reset
[63:0]	ADDRESS	<p>Address Value.</p> <p>The address comparators can support implementations that use multiple address widths. When the trace unit compares the ADDRESS field with an address that has a width less than this field, then the address must be zero-extended to the ADDRESS field width. The trace unit then compares all implemented bits. For example, in a system that supports both 32-bit and 64-bit addresses, when the PE is in AArch32 state the comparator must zero-extend the 32-bit address and compare against the full 64 bits that are stored in the TRCACVR&lt;n&gt;. This requires that the trace analyzer always programs all implemented bits of the TRCACVR&lt;n&gt;.</p> <p>The result of writing a value other than all zeros or all ones to ADDRESS at bits[63:P] is an <b>UNKNOWN</b> value, where P is defined as the virtual address size supported by the PE.</p> <p>The result of writing a value of all zeros or all ones to ADDRESS at bits[63:P] is the written value, and a read of the register returns the written value.</p>	64 {x}

### Access

Must be programmed if any of the following are true:

- ext-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- ext-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- ext-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- ext-TRCVISSCTLR.START[n] == 0b1.
- ext-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- ext-TRCQCTLR.RANGE[n/2] == 0b1.

### Accessibility

Must be programmed if any of the following are true:

- ext-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- ext-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- ext-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- ext-TRCVISSCTLR.START[n] == 0b1.

- ext-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- ext-TRCQCTLR.RANGE[n/2] == 0b1.

Component	Offset	Range
ETM	0x400 + (8 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.49 TRCACATR<n>, Address Comparator Access Type Register <n> , n = 0 - 7

Defines the type of access for the corresponding ext-TRCACVR<n> Register. This register configures the context type, Exception levels, alignment, masking that is applied by the address comparator, and how the address comparator behaves when it is one half of an Address Range Comparator.

Configurations

External register TRCACATR<n> bits [63:0] are architecturally mapped to AArch64 System register A.2.8.49 TRCACATR<n>, Address Comparator Access Type Register <n> , n = 0 - 7 on page 1375 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

0x480 + (8 \* n)

Access type

Read

R

Write

W

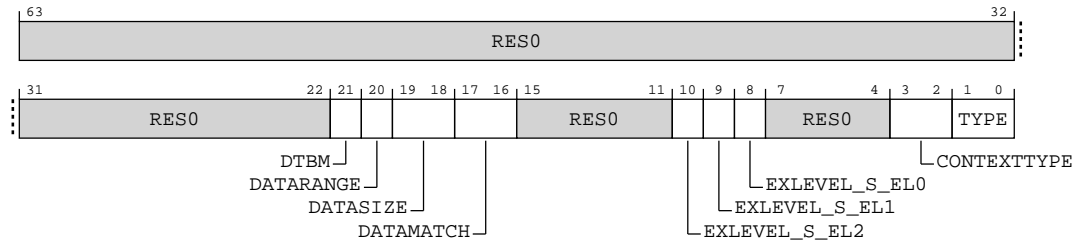
Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-442: EXT\_TRCACATR<n> bit assignments****Table B-863: TRCACATR<n> bit descriptions**

Bits	Name	Description	Reset
[63:22]	RES0	Reserved	RES0
[21]	DTBM	Controls whether data address comparisons use the data address [63:56] bits.  <b>0b0</b> The trace unit ignores the data address [63:56] bits for data address comparisons.  <b>0b1</b> The trace unit uses the data address [63:56] bits for data address comparisons.	x
[20]	DATARANGE	<b>When n == 0 or n == 2</b> Controls whether a data value comparison uses the single address comparator or the address range comparator.  <b>0b0</b> The trace unit uses the single address comparator for data value comparisons. The address range comparator may match at any time. The other single address comparator in the pair is not affected.  <b>0b1</b> The trace unit uses the address range comparator for data value comparisons. The single address comparators in this pair may match at any time.  The trace unit ignores this field when DATAMATCH==0b00.  <b>Otherwise</b> RES0	x



Bits	Name	Description	Reset
[19:18]	DATASIZE	<p><b>When n == 0 or n == 2</b></p> <p>Controls the width of the data value comparison.</p> <p><b>0b00</b> Byte.</p> <p><b>0b01</b> Halfword.</p> <p><b>0b10</b> Word.</p> <p><b>0b11</b> Doubleword.</p> <p><b>Otherwise</b> RES0</p>	xx
[17:16]	DATAMATCH	<p><b>When n == 0 or n == 2</b></p> <p>Controls how the trace unit performs a data value comparison.</p> <p><b>0b00</b> The trace unit does not perform a data value comparison.</p> <p><b>0b01</b> The trace unit performs a data value comparison. If the data value comparator matches and the address comparator matches, the trace unit signals a match.</p> <p><b>0b10</b> Reserved.</p> <p><b>0b11</b> The trace unit performs a data value comparison. If the data value comparator does not match and the address comparator matches, the trace unit signals a match.</p> <p><b>Otherwise</b> RES0</p>	xx
[15:11]	RES0	Reserved	RES0
[10]	EXLEVEL_S_EL2	<p>Secure EL2 address comparison control. Controls whether a comparison can occur at EL2 in Secure state.</p> <p><b>0b0</b> The address comparator performs comparisons in Secure EL2.</p> <p><b>0b1</b> The address comparator does not perform comparisons in Secure EL2.</p>	x
[9]	EXLEVEL_S_EL1	<p>Secure EL1 address comparison control. Controls whether a comparison can occur at EL1 in Secure state.</p> <p><b>0b0</b> The address comparator performs comparisons in Secure EL1.</p> <p><b>0b1</b> The address comparator does not perform comparisons in Secure EL1.</p>	x

Bits	Name	Description	Reset
[8]	EXLEVEL_S_ELO	Secure ELO address comparison control. Controls whether a comparison can occur at ELO in Secure state.  <b>0b0</b> The address comparator performs comparisons in Secure ELO.  <b>0b1</b> The address comparator does not perform comparisons in Secure ELO.	<b>x</b>
[7:4]	RES0	Reserved	<b>RES0</b>
[3:2]	CONTEXTTYPE	Controls whether the address comparator is dependent on a Context Identifier Comparator, a Virtual Context Identifier Comparator, or both comparisons.  <b>0b00</b> The address comparator is not dependent on the Context Identifier Comparator or Virtual Context Identifier Comparator.  <b>0b01</b> The address comparator is dependent on the Context Identifier Comparator. If both the Context Identifier Comparator and the address comparison match, the address comparator signals a match.  <b>0b10</b> The address comparator is dependent on the Virtual Context Identifier Comparator. If both the Virtual Context Identifier Comparator and the address comparison match, the address comparator signals a match.  <b>0b11</b> The address comparator is dependent on the Context Identifier Comparator and Virtual Context Identifier Comparator. If the Context Identifier Comparator, the Virtual Context Identifier Comparator and address comparison all match, the address comparator signals a match.	<b>xx</b>
[1:0]	TYPE	Controls what type of comparison the trace unit performs.  <b>0b00</b> Instruction address.  <b>0b01</b> Data load address.  <b>0b10</b> Data store address.  <b>0b11</b> Data load address or data store address.	<b>xx</b>

## Access

Must be programmed if any of the following are true:

- ext-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- ext-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- ext-TRCVIIECTLR.INCLUDE[n/2] == 0b1.

- ext-TRCVISSCTLR.START[n] == 0b1.
- ext-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- ext-TRCQCTLR.RANGE[n/2] == 0b1.

Accessibility

Must be programmed if any of the following are true:

- ext-TRCBBCTLR.RANGE[n/2] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0100 and TRCRSCTLR<a>.SAC[n] == 0b1.
- TRCRSCTLR<a>.GROUP == 0b0101 and TRCRSCTLR<a>.ARC[n/2] == 0b1.
- ext-TRCVIIECTLR.EXCLUDE[n/2] == 0b1.
- ext-TRCVIIECTLR.INCLUDE[n/2] == 0b1.
- ext-TRCVISSCTLR.START[n] == 0b1.
- ext-TRCVISSCTLR.STOP[n] == 0b1.
- TRCSSCCR<>.ARC[n/2] == 0b1.
- TRCSSCCR<>.SAC[n] == 0b1.
- ext-TRCQCTLR.RANGE[n/2] == 0b1.

Component	Offset	Range
ETM	0x480 + (8 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.50 TRCDVCVR<n>, Data Value Comparator Value Register <n> , n = 0 - 1

Contains a data value.

Configurations

External register TRCDVCVR<n> bits [63:0] are architecturally mapped to AArch64 System register [A.2.8.46 TRCDVCVR<n>, Data Value Comparator Value Register <n> , n = 0 - 1](#) on page 1368 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

0x500 + (16 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-443: EXT\_TRCDVCVR<n> bit assignments

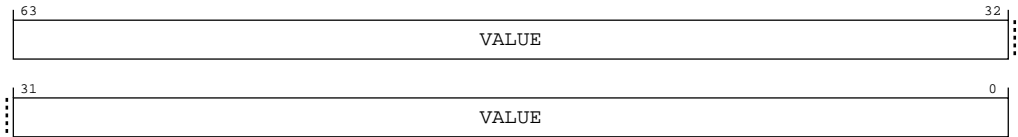


Table B-865: TRCDVCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:0]	VALUE	Data Value.  The data value comparators can support implementations that use multiple data widths. When the trace unit compares the VALUE field with a data value that has a width less than this field, then software must also write the comparison data value to both the upper bits and the lower bits of the VALUE field. For example, in a system that supports both 32-bit and 64-bit data widths, then software must set VALUE[63:32]=VALUE[31:0] if the trace unit is to compare a 32-bit data value.	64 { x }

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

Component	Offset	Range
ETM	0x500 + (16 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.51 TRCDVCMR<n>, Data Value Comparator Mask Register <n> , n = 0 - 1

Contains a data mask value.

Configurations

External register TRCDVCMR<n> bits [63:0] are architecturally mapped to AArch64 System register [A.2.8.47 TRCDVCMR<n>, Data Value Comparator Mask Register <n> , n = 0 - 1](#) on page 1370 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

0x580 + (16 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-444: EXT\_TRCDVCMR<n> bit assignments

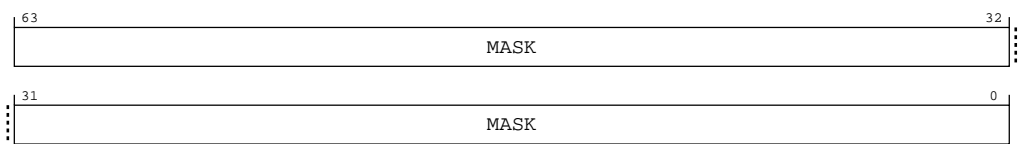


Table B-867: TRCDVCMR<n> bit descriptions

Bits	Name	Description	Reset
[63:0]	MASK	<p>Data mask value.</p> <p>If a bit is set to 1 in the mask then the comparator ignores that bit number for a data value comparison. Software must ensure that the relevant bit in ext-TRCDVCVR&lt;n&gt; is programmed to 0, otherwise the comparator might fail to match.</p> <p>The data value comparators can support implementations that use multiple data widths. When the trace unit compares the ext-TRCDVCVR&lt;n&gt;.VALUE field with a data value that has a width less than this field, then software must also write the data mask value to both the upper bits and the lower bits of the MASK field. For example, in a system that supports both 32-bit and 64-bit data widths, then software must set MASK[63:32]==MASK[31:0] if the trace unit is to compare a 32-bit data value.</p>	64 {x}

Accessibility

Might ignore writes when the trace unit is enabled or not idle.

Component	Offset	Range
ETM	0x580 + (16 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.52 TRCCIDCVR<n>, Context Identifier Comparator Value Registers <n> , n = 0

Contains a Context identifier value.

Configurations

External register TRCCIDCVR<n> bits [63:0] are architecturally mapped to AArch64 System register [A.2.8.52 TRCCIDCVR<n>, Context Identifier Comparator Value Registers <n> , n = 0](#) on page 1385 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

$0x600 + (8 * n)$

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3	0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-445: EXT\_TRCCIDCVR<n> bit assignments

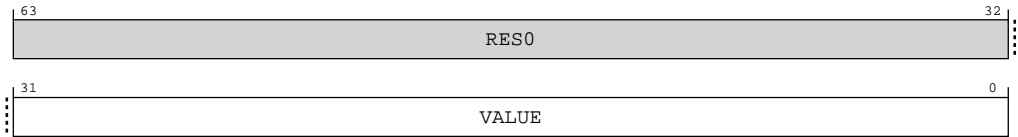


Table B-869: TRCCIDCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	VALUE	Context identifier value. After a PE Reset, the trace unit assumes that the Context identifier is zero until the PE updates the Context identifier.	32 {x}

Access

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0110 and TRCRSCTLR<a>.CID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b01 or 0b11 and TRCACATR<a>.CONTEXT == n.

Accessibility

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0110 and TRCRSCTLR<a>.CID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b01 or 0b11 and TRCACATR<a>.CONTEXT == n.

Component	Offset	Range
ETM	0x600 + (8 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.53 TRCVMIDCVR<n>, Virtual Context Identifier Comparator Value Register <n> , n = 0

Contains the Virtual Context Identifier Comparator value.

Configurations

External register TRCVMIDCVR<n> bits [63:0] are architecturally mapped to AArch64 System register A.2.8.53 TRCVMIDCVR<n>, Virtual Context Identifier Comparator Value Register <n> , n = 0 on page 1387 bits [63:0].

Attributes

Width

64

Component

ETM

Register offset

0x640 + (8 \* n)

Access type

Read

R

Write

W

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Note



Bit descriptions

Figure B-446: EXT\_TRCVMIDCVR<n> bit assignments

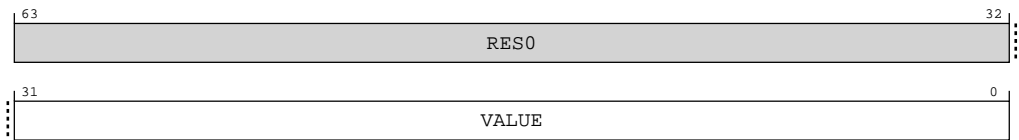


Table B-871: TRCVMIDCVR<n> bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31:0]	VALUE	Virtual context identifier value. After a PE Reset, the trace unit assumes that the Virtual context identifier is zero until the PE updates the Virtual context identifier.	32 {x}

Access

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0111 and TRCRSCTLR<a>.VMID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b10 or 0b11 and TRCACATR<a>.CONTEXT == n.

Accessibility

Must be programmed if any of the following are true:

- TRCRSCTLR<a>.GROUP == 0b0111 and TRCRSCTLR<a>.VMID[n] == 0b1.
- TRCACATR<a>.CONTEXTTYPE == 0b10 or 0b11 and TRCACATR<a>.CONTEXT == n.

Component	Offset	Range
ETM	0x640 + (8 * n)	None

This interface is accessible as follows:

RW

B.2.2.7.54 TRCCIDCCTLR0, Context Identifier Comparator Control Register 0

Contains Context identifier mask values for the ext-TRCCIDCVR<n> registers, for n = 0 to 3.

Configurations

External register TRCCIDCCTLR0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.50 TRCCIDCCTLR0, Context Identifier Comparator Control Register 0](#) on page 1380 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x680

Access type

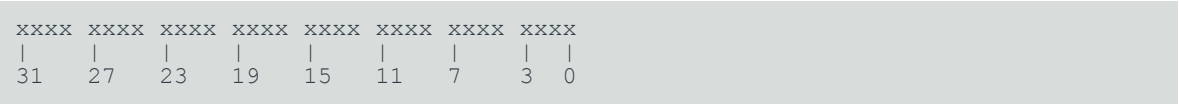
Read

R

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-447: EXT\_TRCCIDCCTLR0 bit assignments

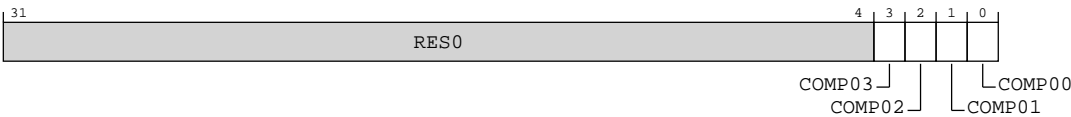


Table B-873: TRCCIDCCTLR0 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	COMP0<m>, bit[m], where m = 3 to 0	<p>TRCCIDCVR0 mask control. Specifies the mask value that the trace unit applies to TRCCIDCVR0. Each bit in this field corresponds to a byte in TRCCIDCVR0.</p> <p><b>0b0</b></p> <p>The trace unit includes TRCCIDCVR0[(m×8+7):(m×8)] when it performs the Context identifier comparison.</p> <p><b>0b1</b></p> <p>The trace unit ignores TRCCIDCVR0[(m×8+7):(m×8)] when it performs the Context identifier comparison.</p>	xxxx

Access

If software uses the ext-TRCCIDCVR<n> registers, for n = 0 to 3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in ext-TRCCIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in ext-TRCCIDCVR<n> is not 0x00, the Context Identifier Comparator will not match.

Accessibility

If software uses the ext-TRCCIDCVR<n> registers, for n = 0 to 3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in ext-TRCCIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in ext-TRCCIDCVR<n> is not 0x00, the Context Identifier Comparator will not match.

Component	Offset	Range
ETM	0x680	None

This interface is accessible as follows:

RW

B.2.2.7.55 TRCVMIDCCTLR0, Virtual Context Identifier Comparator Control Register 0

Virtual Context Identifier Comparator mask values for the ext-TRCVMIDCVR<n> registers, where n=0-3.

Configurations

External register TRCVMIDCCTLR0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.51 TRCVMIDCCTLR0, Virtual Context Identifier Comparator Control Register 0](#) on page 1382 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0x688

Access type

Read  
R  
  
Write  
W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-448: EXT\_TRCVMIDCCTLR0 bit assignments

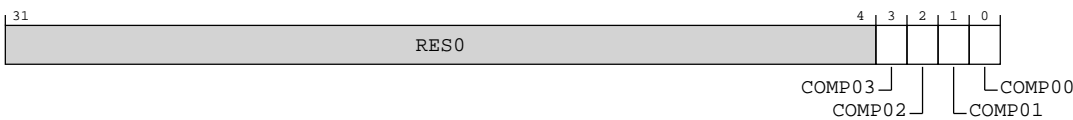


Table B-875: TRCVMIDCCTLR0 bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	COMP0<m>, bit[m], where m = 3 to 0	<p>TRCVMIDCVR0 mask control. Specifies the mask value that the trace unit applies to TRCVMIDCVR0. Each bit in this field corresponds to a byte in TRCVMIDCVR0.</p> <p><b>0b0</b></p> <p>The trace unit includes TRCVMIDCVR0[(m×8+7):(m×8)] when it performs the Virtual context identifier comparison.</p> <p><b>0b1</b></p> <p>The trace unit ignores TRCVMIDCVR0[(m×8+7):(m×8)] when it performs the Virtual context identifier comparison.</p>	xxxx

Access

If software uses the ext-TRCVMIDCVR<n> registers, where n=0-3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in ext-TRCVMIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in ext-TRCVMIDCVR<n> is not 0x00, the Virtual Context Identifier Comparator will not match.

Accessibility

If software uses the ext-TRCVMIDCVR<n> registers, where n=0-3, then it must program this register.

If software sets a mask bit to 0b1 then it must program the relevant byte in ext-TRCVMIDCVR<n> to 0x00.

If any bit is 0b1 and the relevant byte in ext-TRCVMIDCVR<n> is not 0x00, the Virtual Context Identifier Comparator will not match.

Component	Offset	Range
ETM	0x688	None

This interface is accessible as follows:

RW

B.2.2.7.56 TRCITCTRL, Integration Mode Control Register

No functional/integration mode switching implemented in the trace unit.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xF00

Access type

RW

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-449: EXT\_TRCITCTRL bit assignments

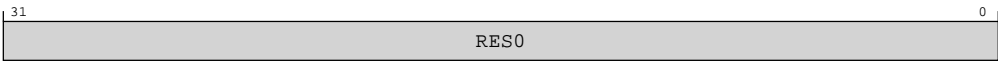


Table B-877: TRCITCTRL bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0xF00	None

This interface is accessible as follows:

RW

B.2.2.7.57 TRCCLAIMSET, Claim Tag Set Register

In conjunction with ext-TRCCLAIMCLR, provides Claim Tag bits that can be separately set and cleared to indicate whether functionality is in use by a debug agent.

Configurations

External register TRCCLAIMSET bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.55 TRCCLAIMSET, Claim Tag Set Register](#) on page 1390 bits [31:0].

Attributes

Width

32

Component

ETM

Register offset

0xFA0

Access type

RAOW1S

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-450: EXT\_TRCCLAIMSET bit assignments

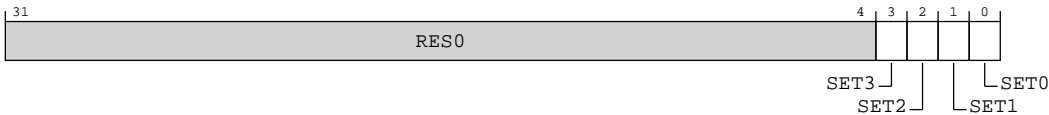


Table B-879: TRCCLAIMSET bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	SET<m>, bit[m], where m = 3 to 0	<p>Claim Tag Set. Indicates whether Claim Tag bit m is implemented, and is used to set Claim Tag bit m to 0b1.</p> <p><b>0b0</b></p> <p>On a read: Claim Tag bit m is not implemented.</p> <p>On a write: Ignored.</p> <p><b>0b1</b></p> <p>On a read: Claim Tag bit m is implemented.</p> <p>On a write: Set Claim Tag bit m to 0b1.</p>	0b1111

Accessibility

Component	Offset	Range
ETM	0xFA0	None

This interface is accessible as follows:

RW

B.2.2.7.58 TRCCLAIMCLR, Claim Tag Clear Register

In conjunction with ext-TRCCLAIMSET, provides Claim Tag bits that can be separately set and cleared to indicate whether functionality is in use by a debug agent.

Configurations

External register TRCCLAIMCLR bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.56 TRCCLAIMCLR, Claim Tag Clear Register](#) on page 1392 bits [31:0].

Attributes

Width  
32

Component  
ETM

Register offset  
0xFA4

Access type  
RW1C

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-451: EXT\_TRCCLAIMCLR bit assignments

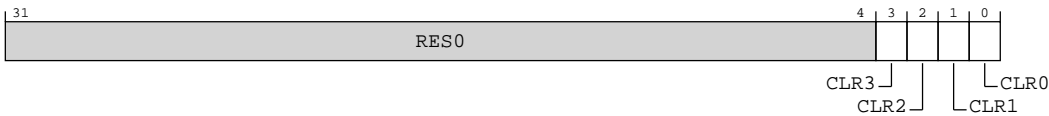


Table B-881: TRCCLAIMCLR bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	CLR<m>, bit[m], where m = 3 to 0	<p>Claim Tag Clear. Indicates the current status of the Claim Tag bit m, and is used to clear Claim Tag bit m to 0b0.</p> <p><b>0b0</b></p> <p>On a read: Claim Tag bit m is not set.</p> <p>On a write: Ignored.</p> <p><b>0b1</b></p> <p>On a read: Claim Tag bit m is set.</p> <p>On a write: Clear Claim tag bit m to 0b0.</p> <p>The number of Claim Tag bits implemented is indicated in ext-TRCCLAIMSET.</p>	xxxx



Accessibility

Component	Offset	Range
ETM	0xFA4	None

This interface is accessible as follows:

RW

B.2.2.7.59 TRCDEVAFF, Device Affinity Register

Reads the same value as the AArch64-MPIDR\_EL1 register for the PE this trace unit has affinity with.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

ETM

Register offset

0xFA8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-452: EXT\_TRCDEVAFF bit assignments

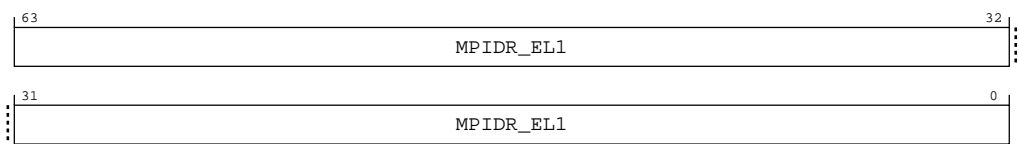


Table B-883: TRCDEVAFF bit descriptions

Bits	Name	Description	Reset
[63:0]	MPIDR_EL1	Read-only copy of AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.	64 {x}

Accessibility

Component	Offset	Range
ETM	0xFA8	None

This interface is accessible as follows:

RO

B.2.2.7.60 TRCLAR, Lock Access Register

Legacy Software Lock mechanism.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFB0

Access type

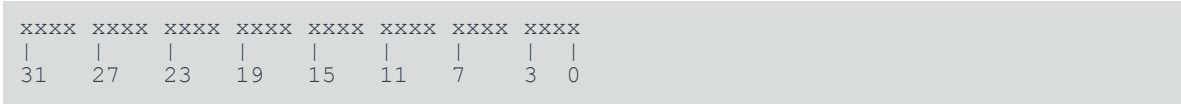
Read

RESERVED

Write

W

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-453: EXT\_TRCLAR bit assignments

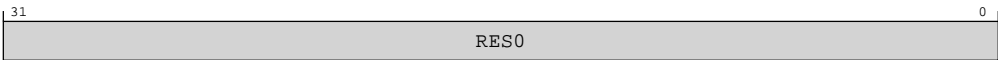


Table B-885: TRCLAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Software Lock not implemented, writes to TRCLAR are ignored.

Component	Offset	Range
ETM	0xFB0	None

This interface is accessible as follows:

WO

B.2.2.7.61 TRCLSR, Lock Status Register

Legacy Software Lock mechanism.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

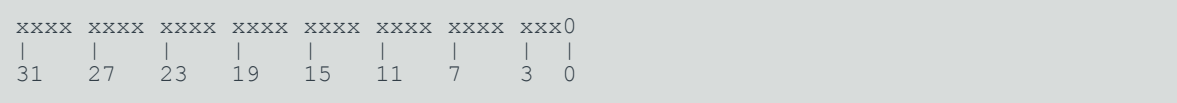
Register offset

0xFB4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-454: EXT\_TRCLSR bit assignments

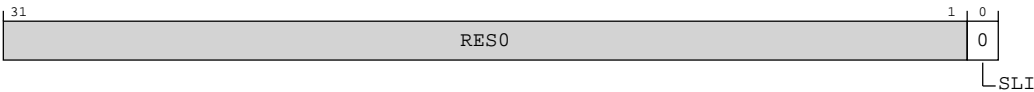


Table B-887: TRCLSR bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0
[0]	SLI	Indicates whether the Software Lock is implemented.  0b0  Software Lock is not implemented. Writes to the ext-TRCLAR are ignored.	0b0

Accessibility

Component	Offset	Range
ETM	0xFB4	None

This interface is accessible as follows:

RO

B.2.2.7.62 TRCAUTHSTATUS, Authentication Status Register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for debug.

Configurations

External register TRCAUTHSTATUS bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.57 TRCAUTHSTATUS, Authentication Status Register](#) on page 1394 bits [31:0].

Attributes

- Width32
- ComponentETM
- Register offset0xFB8
- Access typeRO
- Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-455: EXT\_TRCAUTHSTATUS bit assignments

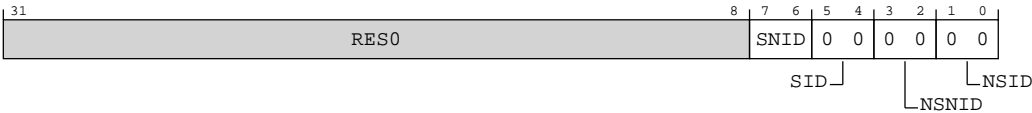


Table B-889: TRCAUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:6]	SNID	Secure Non-invasive Debug. Indicates whether Secure non-invasive debug features are implemented and enabled.  <b>0b10</b> Secure Non-invasive Debug implemented and disabled.  <b>0b11</b> Secure Non-invasive Debug implemented and enabled.	xx
[5:4]	SID	Secure Invasive Debug. Indicates whether Secure invasive debug features are implemented and enabled.  <b>0b00</b> Secure invasive debug features not implemented.	0b00
[3:2]	NSNID	Non-secure Non-invasive Debug. Indicates whether Non-secure non-invasive debug features are implemented and enabled.  <b>0b00</b> Non-secure non-invasive debug features not implemented.	0b00
[1:0]	NSID	Non-secure Invasive Debug. Indicates whether Non-secure invasive debug features are implemented and enabled.  <b>0b00</b> Non-secure invasive debug features not implemented.	0b00

### Accessibility

Component	Offset	Range
ETM	0xFB8	None

This interface is accessible as follows:

RO

#### B.2.2.7.63 TRCDEVARCH, Device Architecture Register

Provides discovery information for the component.

### Configurations

External register TRCDEVARCH bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.58 TRCDEVARCH, Device Architecture Register](#) on page 1396 bits [31:0].

### Attributes

#### Width

32

#### Component

ETM

#### Register offset

0xFBC

#### Access type

RO

Reset value

0100 0111 0111 0101 0100 1010 0001 0011

Bit descriptions

Figure B-456: EXT\_TRCDEVARCH bit assignments

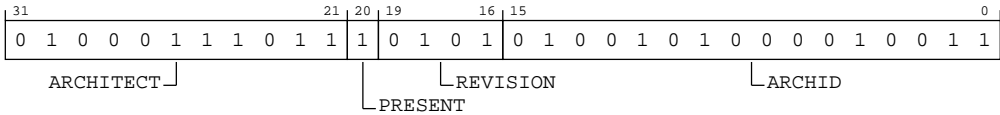


Table B-891: TRCDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Architect. Defines the architect of the component. <b>0b01000111011</b> JEP106 continuation code 0x4, ID code 0x3B. Arm Limited.	0b01000111011
[20]	PRESENT	DEVARCH Present. Defines that the DEVARCH register is present. <b>0b1</b> Device Architecture information present.	0b1
[19:16]	REVISION	Revision. Defines the architecture revision of the component. <b>0b0101</b> ETMv4.5.	0b0101
[15:0]	ARCHID	Architecture ID. <b>0b0100101000010011</b> Arm PE Trace architecture ETMv4.	0x4A13

Accessibility

Component	Offset	Range
ETM	0xFBC	None

This interface is accessible as follows:

RO

B.2.2.7.64 TRCDEVID, Device Configuration Register

Provides discovery information for the component.

Configurations

External register TRCDEVID bits [31:0] are architecturally mapped to AArch64 System register [A.2.8.54 TRCDEVID, Device Configuration Register](#) on page 1389 bits [31:0].

Attributes

Width

32

Component

ETM

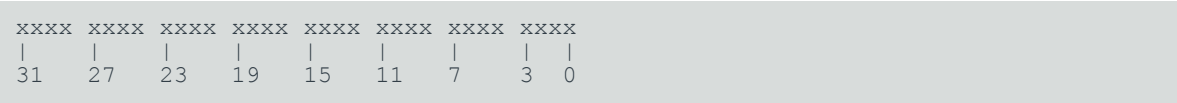
Register offset

0xFC8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-457: EXT\_TRCDEVID bit assignments

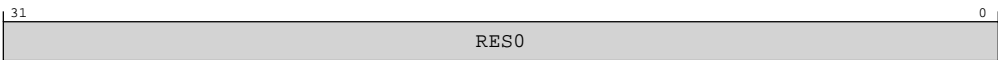


Table B-893: TRCDEVID bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0xFC8	None

This interface is accessible as follows:

RO



B.2.2.7.65 TRCDEVTYPE, Device Type Register

Provides discovery information for the component. If the part number field is not recognised, a debugger can report the information that is provided by TRCDEVTYPE about the component instead.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

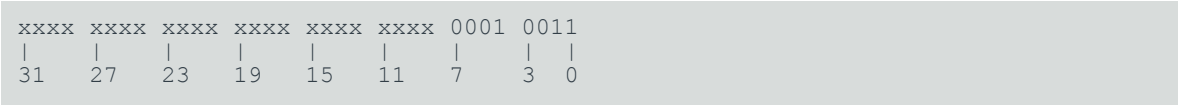
Register offset

0xFCC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-458: EXT\_TRCDEVTYPE bit assignments

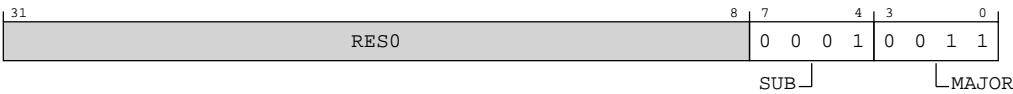


Table B-895: TRCDEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Component sub-type.  0b0001 Trace source associated with a PE.	0b0001

Bits	Name	Description	Reset
[3:0]	MAJOR	Component major type.  <b>0b0011</b> Trace source.	0b0011

Accessibility

Component	Offset	Range
ETM	0xFCC	None

This interface is accessible as follows:

RO

B.2.2.7.66 TRCPIDR4, Peripheral Identification Register 4

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFD0

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0100
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-459: EXT\_TRCPIDR4 bit assignments

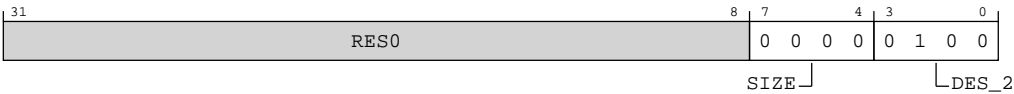


Table B-897: TRCPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SIZE	4KB count. <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	JEP106 continuation code. <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Range
ETM	0xFD0	None

This interface is accessible as follows:

RO

B.2.2.7.67 TRCPIDR5, Peripheral Identification Register 5

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

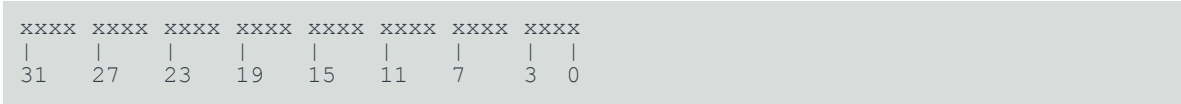
Register offset

0xFD4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-460: EXT\_TRCPIDR5 bit assignments



Table B-899: TRCPIDR5 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0xFD4	None

This interface is accessible as follows:

RO

B.2.2.7.68 TRCPIDR6, Peripheral Identification Register 6

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFD8

Access type  
RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-461: EXT\_TRCPIDR6 bit assignments



Table B-901: TRCPIDR6 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0xFD8	None

This interface is accessible as follows:

RO

B.2.2.7.69 TRCPIDR7, Peripheral Identification Register 7

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFDC

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-462: EXT\_TRCPIDR7 bit assignments



Table B-903: TRCPIDR7 bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Range
ETM	0xFDC	None

This interface is accessible as follows:

RO

B.2.2.7.70 TRCPIDR0, Peripheral Identification Register 0

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFE0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-463: EXT\_TRCPIDR0 bit assignments

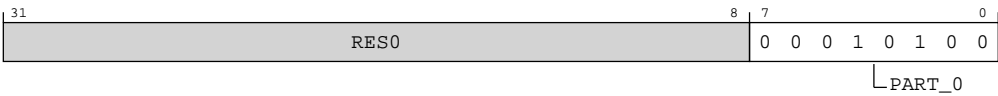


Table B-905: TRCPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b00010100 Cortex-R82AE trace unit. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Range
ETM	0xFE0	None

This interface is accessible as follows:

RO

B.2.2.7.71 TRCPIDR1, Peripheral Identification Register 1

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFE4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-464: EXT\_TRCPIDR1 bit assignments

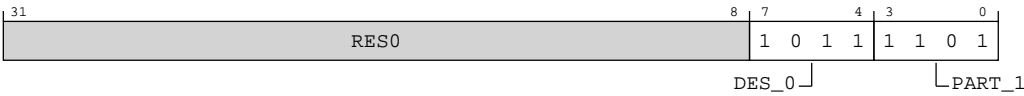


Table B-907: TRCPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	JEP106 identification code bits [3:0].  0b1011 Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8].  0b1101 Cortex-R82AE trace unit. Bits [11:8] of part number 0xD14.	0b1101



Accessibility

Component	Offset	Range
ETM	0xFE4	None

This interface is accessible as follows:

RO

B.2.2.7.72 TRCPIDR2, Peripheral Identification Register 2

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFE8

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0111	1011
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-465: EXT\_TRCPIDR2 bit assignments

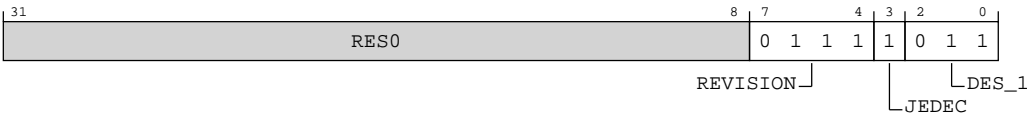


Table B-909: TRCPIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Range
ETM	0xFE8	None

This interface is accessible as follows:

RO

B.2.2.7.73 TRCPIDR3, Peripheral Identification Register 3

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFEC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-466: EXT\_TRCPIDR3 bit assignments



Table B-911: TRCPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Minor errata fixes.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer Modified.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Range
ETM	0xFEC	None

This interface is accessible as follows:

RO

B.2.2.7.74 TRCCIDR0, Component Identification Register 0

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

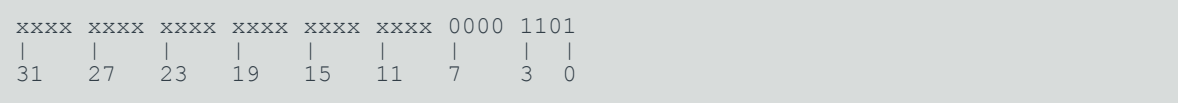
Register offset

0xFF0

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-467: EXT\_TRCCIDR0 bit assignments



Table B-913: TRCCIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble.  0b00001101 CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Range
ETM	0xFF0	None

This interface is accessible as follows:

RO

B.2.2.7.75 TRCCIDR1, Component Identification Register 1

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

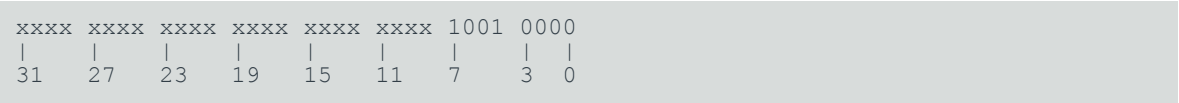
Register offset

0xFF4

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-468: EXT\_TRCCIDR1 bit assignments



Table B-915: TRCCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	CLASS	Component class. <b>0b1001</b> CoreSight debug component.	0b1001
[3:0]	PRMBL_1	Preamble. <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Range
ETM	0xFF4	None

This interface is accessible as follows:

RO

B.2.2.7.76 TRCCIDR2, Component Identification Register 2

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFF8

Access type

RO

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-469: EXT\_TRCCIDR2 bit assignments

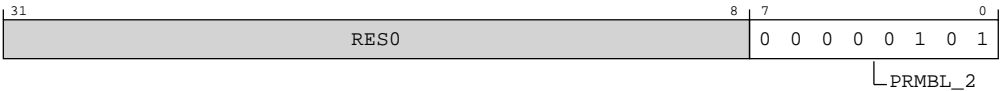


Table B-917: TRCCIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble.  0b00000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Range
ETM	0xFF8	None

This interface is accessible as follows:

RO

B.2.2.7.77 TRCCIDR3, Component Identification Register 3

Provides discovery information for the component.

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

ETM

Register offset

0xFFC

Access type

RO

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1011	0001
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-470: EXT\_TRCCIDR3 bit assignments

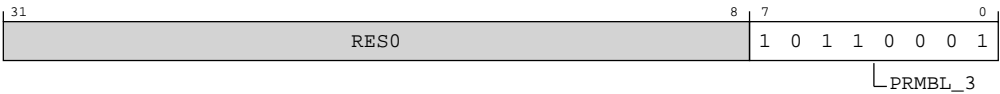


Table B-919: TRCCIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble.  <b>0b10110001</b> CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Range
ETM	0xFFC	None

This interface is accessible as follows:

RO

B.2.2.8 External PMU register description

This section includes the register descriptions for all memory-mapped *Performance Monitoring Unit* (PMU) registers that are accessed for each core.

B.2.2.8.1 PMEVCNTR<n>\_ELO, Performance Monitors Event Count Registers, n = 0 - 5

Holds event counter <n>, which counts events, where <n> is 0 to 30.

Configurations

PMEVCNTR<n>\_ELO is in the Core power domain.

External register PMEVCNTR<n>\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.32 PMEVCNTR<n>\\_ELO, Performance Monitors Event Count Registers, n = 0 - 5](#) on page 848 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0x000 + (8 \* n)

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-471: PMU\_PMEVCNTR<n>\_ELO bit assignments

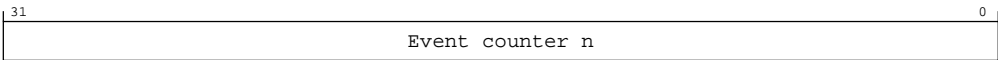


Table B-921: PMEVCNTR<n>\_ELO bit descriptions

Bits	Name	Description	Reset
[31:0]	None	Event counter n. Value of event counter n, where n is the number of this register and is a number from 0 to 30.	32 { x }

Accessibility

Component	Offset	Instance	Range
PMU	0x000 + (8 * n)	PMEVCNTR<n>_ELO	31:0

B.2.2.8.2 PMCCNTR\_ELO, Performance Monitors Cycle Counter

Holds the value of the processor Cycle Counter, CCNT, that counts processor clock cycles. For more information, see *Time as measured by the Performance Monitors cycle counter* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

PMU.PMCCFILTR\_ELO determines the modes and states in which the PMCCNTR\_ELO can increment.

Configurations

PMCCNTR\_ELO is in the Core power domain.

External register PMCCNTR\_ELO bits [63:0] are architecturally mapped to AArch64 System register [A.2.3.27 PMCCNTR\\_ELO, Performance Monitors Cycle Count Register](#) on page 835 bits [63:0].

Attributes

Width

64

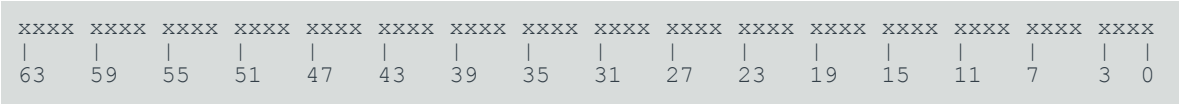
Component

PMU

Register offsets (2)

0x0F8,0x0FC

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-472: PMU\_PMCNTR\_ELO bit assignments

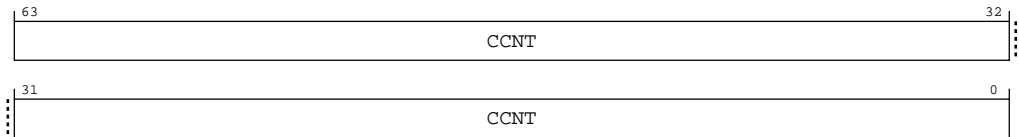


Table B-923: PMCCNTR\_ELO bit descriptions

Bits	Name	Description	Reset
[63:0]	CCNT	Cycle count. Depending on the values of PMU.PMCR_ELO.{LC,D}, the cycle count increments in one of the following ways: <ul style="list-style-type: none"><li>Every processor clock cycle.</li><li>Every 64th processor clock cycle.</li></ul> Writing 1 to PMU.PMCR_ELO.C sets this field to 0.	64 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0x0F8	PMCCNTR_ELO	31:0

Component	Offset	Instance	Range
PMU	0x0FC	PMCCNTR_ELO	63:32

B.2.2.8.3 PMPCSR, Program Counter Sample Register

Holds a sampled instruction address value.

Configurations

This register is available in all configurations.

Attributes

Width

64

Component

PMU

Register offsets (4)

0x200,0x204,0x220,0x224

Reset value

0xxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-473: PMU\_PMPCSR bit assignments

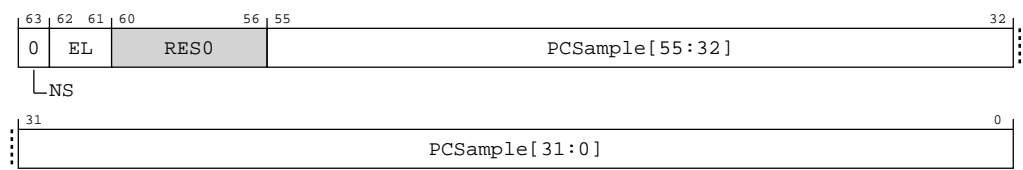


Table B-926: PMPCSR bit descriptions

Bits	Name	Description	Reset
[63]	NS	Non-secure state sample. Indicates the Security state that is associated with the most recent PMPCSR sample or, when it is read as a single atomic 64-bit read, the current PMPCSR sample.  If EL3 is not implemented, this bit indicates the Effective value of SCR.NS.  <b>0b0</b> Sample is from Secure state.	0b0
[62:61]	EL	Exception level status sample. Indicates the Exception level that is associated with the most recent PMPCSR sample or, when it is read as a single atomic 64-bit read, the current PMPCSR sample.  <b>0b00</b> Sample is from EL0.  <b>0b01</b> Sample is from EL1.  <b>0b10</b> Sample is from EL2.	xx
[60:56]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[55:32]	PCSample[55:32]	Bits[55:32] of the sampled instruction address value. The translation regime that PMPCSR samples can be determined from PMPCSR.{NS,EL}.	24 {x}
[31:0]	PCSample[31:0]	<p>Bits[31:0] of the sampled instruction address value.</p> <p>PMPCSR[31:0] reads as 0xFFFFFFFF when any of the following are true:</p> <ul style="list-style-type: none"> <li>The PE is in Debug state.</li> <li>PC Sample-based profiling is prohibited.</li> </ul> <p>If a branch instruction has retired since the PE left reset state, then the first read of PMPCSR[31:0] is permitted but not required to return 0xFFFFFFFF.</p> <p>PMPCSR[31:0] reads as an <b>UNKNOWN</b> value when any of the following are true:</p> <ul style="list-style-type: none"> <li>The PE is in reset state.</li> <li>No branch instruction has retired since the PE left reset state, Debug state, or a state where PC Sample-based Profiling is prohibited.</li> <li>No branch instruction has retired since the last read of PMPCSR[31:0].</li> </ul> <p>For the cases where a read of PMPCSR[31:0] returns 0xFFFFFFFF or an <b>UNKNOWN</b> value, the read has the side-effect of setting PMPCSR[63:32], ext-PMCID1SR, ext-PMCID2SR, and ext-PMVIDSR to <b>UNKNOWN</b> values.</p> <p>Otherwise, a read of PMPCSR[31:0] returns bits [31:0] of the sampled instruction address value and has the side-effect of indirectly writing to PMPCSR[63:32], ext-PMCID1SR, ext-PMCID2SR, and ext-PMVIDSR. The translation regime that PMPCSR samples can be determined from PMPCSR.{NS,EL}.</p>	32 {x}

## Access

IMPLEMENTATION DEFINED extensions to external debug might make the value of this register **UNKNOWN**, see *Permitted behavior that might make the PC Sample-based profiling registers UNKNOWN* in the [Arm® Architecture Reference Manual for A-profile architecture](#).



Note

A 32-bit access to PMPCSR[63:32] does not update the PC sample registers. Only a 64-bit access to PMPCSR[63:0] or a 32-bit access to PMPCSR[31:0] updates the PC sample registers. This includes the value a subsequent 32-bit read of PMPCSR[63:32] will return.

## Accessibility

IMPLEMENTATION DEFINED extensions to external debug might make the value of this register **UNKNOWN**, see 'Permitted behavior that might make the PC Sample-based profiling registers UNKNOWN'.



Note

A 32-bit access to PMPCSR[63:32] does not update the PC sample registers. Only a 64-bit access to PMPCSR[63:0] or a 32-bit access to PMPCSR[31:0] updates the PC sample registers. This includes the value a subsequent 32-bit read of PMPCSR[63:32] will return.

Component	Offset	Instance	Range
PMU	0x200	PMPCSR	31:0

Component	Offset	Instance	Range
PMU	0x204	PMPCSR	63:32

Component	Offset	Instance	Range
PMU	0x220	PMPCSR	31:0

Component	Offset	Instance	Range
PMU	0x224	PMPCSR	63:32

B.2.2.8.4 PMCID1SR, CONTEXTIDR\_EL1 Sample Register

Contains the sampled value of AArch64-CONTEXTIDR\_EL1, captured on reading PMU.PMPCSR[31:0].

Configurations

This register is available in all configurations.

Attributes

Width

32

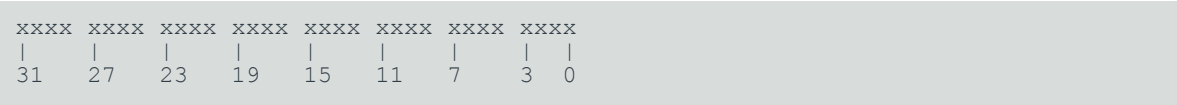
Component

PMU

Register offsets (2)

0x208,0x228

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-474: PMU\_PMCID1SR bit assignments



Table B-931: PMCID1SR bit descriptions

Bits	Name	Description	Reset
[31:0]	CONTEXTIDR_EL1	<div>Context ID. The value of CONTEXTIDR that is associated with the most recent PMU.PMPCSR sample. When the most recent PMU.PMPCSR sample is generated:<ul style="list-style-type: none"><li>If EL1 is using AArch64, then the Context ID is sampled from AArch64-CONTEXTIDR_EL1.</li></ul>Because the value written to this register is an indirect read of CONTEXTIDR, it is <b>CONSTRAINED UNPREDICTABLE</b> whether this register is set to the original or new value if PMU.PMPCSR samples:<ul style="list-style-type: none"><li>An instruction that writes to CONTEXTIDR.</li><li>The next Context synchronization event.</li><li>Any instruction executed between these two instructions.</li></ul></div>	32 {x}

Accessibility

IMPLEMENTATION DEFINED extensions to external debug might make the value of this register UNKNOWN, see 'Permitted behavior that might make the PC Sample-based profiling registers UNKNOWN'.

Component	Offset	Instance	Range
PMU	0x208	PMCID1SR	None

Component	Offset	Instance	Range
PMU	0x228	PMCID1SR	None

B.2.2.8.5 PMVIDSR, VMID Sample Register

Contains the sampled VMID value that is captured on reading PMU.PMPCSR[31:0].

Configurations

This register is available in all configurations.

Attributes

Width

32

Component

PMU

Register offset

0x20C

Reset value





Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-475: PMU\_PMVIDSR bit assignments**



**Table B-934: PMVIDSR bit descriptions**

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	VMID	<p>VMID sample. The VMID associated with the most recent PMU.PMPCSR sample. When the most recent PMU.PMPCSR sample was generated:</p> <ul style="list-style-type: none"> <li>This field is set to an <b>UNKNOWN</b> value if any of the following apply: <ul style="list-style-type: none"> <li>The PE is executing at EL2.</li> </ul> </li> <li>Otherwise: <ul style="list-style-type: none"> <li>If EL2 is using AArch64, this field is set to AArch64-VSCTLR_EL2.VMID.</li> </ul> </li> </ul> <p>Because the value written to PMVIDSR is an indirect read of the VMID value, it is <b>CONSTRAINED UNPREDICTABLE</b> whether PMVIDSR is set to the original or new value if PMU.PMPCSR samples:</p> <ul style="list-style-type: none"> <li>An instruction that writes to the VMID value.</li> <li>The next Context synchronization event.</li> <li>Any instruction executed between these two instructions.</li> </ul>	8 {x}

## Accessibility

IMPLEMENTATION DEFINED extensions to external debug might make the value of this register UNKNOWN, see 'Permitted behavior that might make the PC Sample-based profiling registers UNKNOWN'.

Component	Offset	Instance	Range
PMU	0x20C	PMVIDSR	None

### B.2.2.8.6 PMCID2SR, CONTEXTIDR\_EL2 Sample Register

Contains the sampled value of AArch64-CONTEXTIDR\_EL2, captured on reading PMU.PMPCSR[31:0].

## Configurations

This register is available in all configurations.

## Attributes

## Width

32

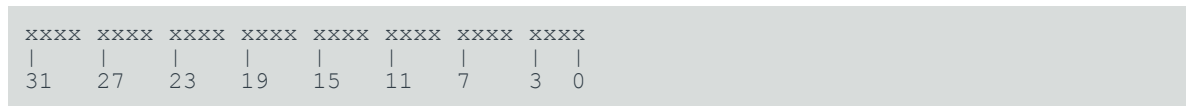
## Component

PMU

## Register offset

0x22C

## Reset value



### Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure B-476: PMU\_PMCID2SR bit assignments



### Table B-936: PMCID2SR bit descriptions

Bits	Name	Description	Reset
[31:0]	CONTEXTIDR_EL2	<p>Context ID. The value of AArch64-CONTEXTIDR_EL2 that is associated with the most recent PMU.PMPCSR sample. When the most recent PMU.PMPCSR sample is generated:</p> <ul style="list-style-type: none"> <li>If the PE is not executing at EL3, EL2 is using AArch64, and EL2 is enabled in the current Security state, then this field is set to the Context ID sampled from AArch64-CONTEXTIDR_EL2.</li> <li>Otherwise, this field is set to an <b>UNKNOWN</b> value.</li> </ul> <p>Because the value written to this field is an indirect read of AArch64-CONTEXTIDR_EL2, it is CONSTRAINED UNPREDICTABLE whether this field is set to the original or new value if PMU.PMPCSR samples:</p> <ul style="list-style-type: none"> <li>An instruction that writes to AArch64-CONTEXTIDR_EL2.</li> <li>The next Context synchronization event.</li> <li>Any instruction executed between these two instructions.</li> </ul>	32 {x}

## Accessibility

IMPLEMENTATION DEFINED extensions to external debug might make the value of this register UNKNOWN, see 'Permitted behavior that might make the PC Sample-based profiling registers UNKNOWN'.



Component	Offset	Instance	Range
PMU	0x22C	PMCID2SR	None

B.2.2.8.7    [PMEVTYPER<n>\\_ELO, Performance Monitors Event Type Registers, n = 0 - 5](#)

Configures event counter <n>, where <n> is 0 to 30.

Configurations

PMEVTYPER<n>\_ELO is in the Core power domain.

If event counter n is not implemented:

- When `IsCorePowered()` && `!DoubleLockStatus()` && `!OSLockStatus()` && `AllowExternalPMUAccess()`, accesses are RES0.
- Otherwise, it is CONSTRAINED UNPREDICTABLE whether accesses to this register are RES0 or generate an error response.

External register PMEVTYPER<n>\_ELO bits [63:0] are architecturally mapped to AArch64 System register [A.2.3.33 PMEVTYPER<n>\\_ELO, Performance Monitors Event Type Registers, n = 0 - 5](#) on page 851 bits [63:0].

Attributes

Width

64

Component

PMU

Register offset

0x400 + (4 \* n)

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
															0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-477: PMU\_PMEVTYPER<n>\_ELO bit assignments

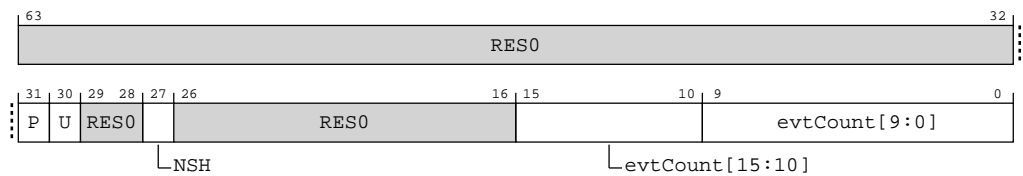


Table B-938: PMEVTYPER<n>\_ELO bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	P	EL1 filtering. Controls counting events in EL1.  <b>0b0</b> This field has no effect on filtering of events.  <b>0b1</b> Events in EL1 are not counted.	x
[30]	U	ELO filtering. Controls counting events in ELO.  <b>0b0</b> This field has no effect on filtering of events.  <b>0b1</b> Events in ELO are not counted.	x
[29:28]	RES0	Reserved	RES0
[27]	NSH	EL2 filtering. Controls counting events in EL2.  <b>0b0</b> Events in EL2 are not counted.  <b>0b1</b> This field has no effect on filtering of events.	x
[26:16]	RES0	Reserved	RES0
[15:10]	evtCount[15:10]	Extension to evtCount[9:0]. For more information, see evtCount[9:0].	6 { x }

Bits	Name	Description	Reset
[9:0]	evtCount[9:0]	<p>Event to count. The event number of the event that is counted by event counter PMU.PMEVCNTR&lt;n&gt;_ELO.</p> <p>Software must program this field with an event that is supported by the PE being programmed.</p> <p>The ranges of event numbers allocated to each type of event are shown in <i>Allocation of the PMU event number space</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p> <p>If FEAT_PMUv3p8 is implemented and PMEVTYPER&lt;n&gt;_ELO.evtCount is programmed to an event that is reserved or not supported by the PE, no events are counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is the value written to the field.</p> <p><b>Note:</b> Arm recommends this behavior for all implementations of FEAT_PMUv3.</p> <p>Otherwise, if PMEVTYPER&lt;n&gt;_ELO.evtCount is programmed to an event that is reserved or not supported by the PE, the behavior depends on the value written:</p> <ul style="list-style-type: none"> <li>For the range 0x0000 to 0x003F, no events are counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is the value written to the field.</li> <li>If FEAT_PMUv3p1 is implemented, for the range 0x4000 to 0x403F, no events are counted and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is the value written to the field.</li> <li>For other values, it is UNPREDICTABLE what event, if any, is counted, and the value returned by a direct or external read of the PMEVTYPER&lt;n&gt;_ELO.evtCount field is <b>UNKNOWN</b>.</li> </ul> <p><b>Note:</b> UNPREDICTABLE means the event must not expose privileged information.</p>	10 {x}

## Accessibility

Component	Offset	Instance	Range
PMU	0x400 + (4 * n)	PMEVTYPER<n>_ELO	31:0

### B.2.2.8.8 PMCCFILTR\_ELO, Performance Monitors Cycle Counter Filter Register

Determines the modes in which the Cycle Counter, PMU.PMCCNTR\_ELO, increments.

## Configurations

PMCCFILTR\_ELO is in the Core power domain.

On a Warm or Cold reset, RW fields in this register reset to:

- Architecturally UNKNOWN values if the reset is to an Exception level that is using AArch64.

The register is not affected by an External debug reset.

External register PMCCFILTR\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.34 PMCCFILTR\\_ELO, Performance Monitors Cycle Count Filter Register](#) on page 854 bits [31:0].

Attributes

Width

64

Component

PMU

Register offset

0x47C

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-478: PMU\_PMCCFILTR\_EL0 bit assignments

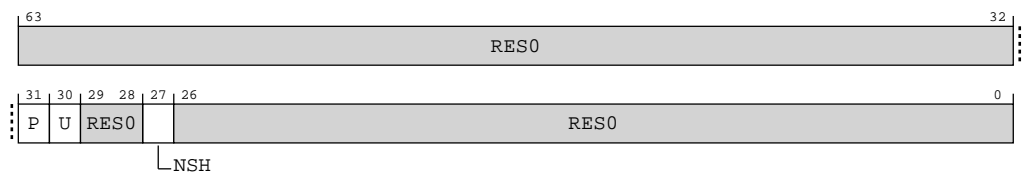


Table B-940: PMCCFILTR\_EL0 bit descriptions

Bits	Name	Description	Reset
[63:32]	RES0	Reserved	RES0
[31]	P	EL1 filtering. Controls counting cycles in EL1.  <b>0b0</b> This field has no effect on filtering of cycles.  <b>0b1</b> Cycles in EL1 are not counted.	x
[30]	U	ELO filtering. Controls counting cycles in EL0.  <b>0b0</b> This field has no effect on filtering of cycles.  <b>0b1</b> Cycles in EL0 are not counted.	x
[29:28]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[27]	NSH	EL2 filtering. Controls counting cycles in EL2.  <b>0b0</b> Cycles in EL2 are not counted.  <b>0b1</b> This field has no effect on filtering of cycles.	x
[26:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
PMU	0x47C	PMCCFILTR_ELO	31:0

B.2.2.8.9     [PMCNTENSET\\_ELO, Performance Monitors Count Enable Set Register](#)

Enables the Cycle Count Register, PMU.PMCCNTR\_ELO, and any implemented event counters PMU.PMEVCNTR<n>\_ELO. Reading this register shows which counters are enabled.

Configurations

PMCNTENSET\_ELO is in the Core power domain.

External register PMCNTENSET\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.20 PMCNTENSET\\_ELO, Performance Monitors Count Enable Set Register](#) on page 805 bits [31:0].

External register PMCNTENSET\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.21 PMCNTENCLR\\_ELO, Performance Monitors Count Enable Clear Register](#) on page 808 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xC00

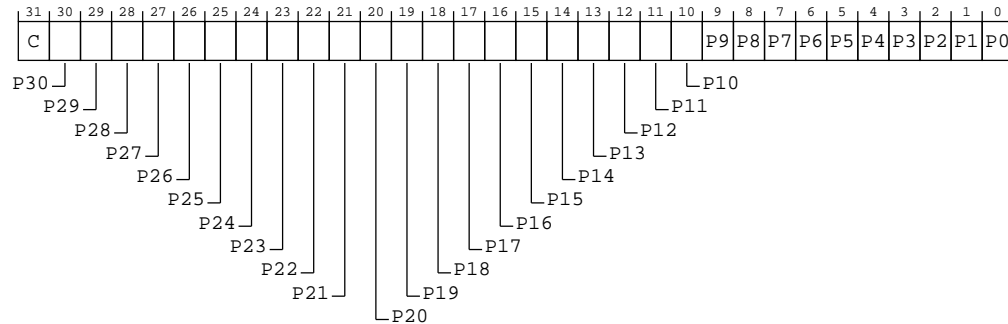
Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0

**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-479: PMU\_PMCNTENSET\_ELO bit assignments****Table B-942: PMCNTENSET\_ELO bit descriptions**

Bits	Name	Description	Reset
[31]	C	<p>PMU.PMCCNTR_ELO enable. On writes, allows software to enable PMU.PMCCNTR_ELO. On reads, returns the PMU.PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>PMU.PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>PMU.PMCCNTR_ELO enabled.</p> <p>Access to this field is: W1S</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>PMEVCNTR&lt;m&gt;_ELO enable. On writes, allows software to enable PMEVCNTR&lt;m&gt;_ELO. On reads, returns the PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p><b>When m &gt;= 6</b></p> <p>Access to this field is: <b>RAZ/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: W1S</p>	31 {x}

## Accessibility

Component	Offset	Instance	Range
PMU	0xC00	PMCNTENSET_ELO	31:0

B.2.2.8.10    [PMCNTENCLR\\_ELO, Performance Monitors Count Enable Clear Register](#)

Disables the Cycle Count Register, PMU.PMCCNTR\_ELO, and any implemented event counters AArch32-PMEVCNTR<n>. Reading this register shows which counters are enabled.

**Configurations**

PMCNTENCLR\_ELO is in the Core power domain.

External register PMCNTENCLR\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.21 PMCNTENCLR\\_ELO, Performance Monitors Count Enable Clear Register](#) on page 808 bits [31:0].

External register PMCNTENCLR\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.20 PMCNTENSET\\_ELO, Performance Monitors Count Enable Set Register](#) on page 805 bits [31:0].

**Attributes**

**Width**

32

**Component**

PMU

**Register offset**

0xC20

**Reset value**

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



**Note**

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-480: PMU\_PMCNTENCLR\_ELO bit assignments

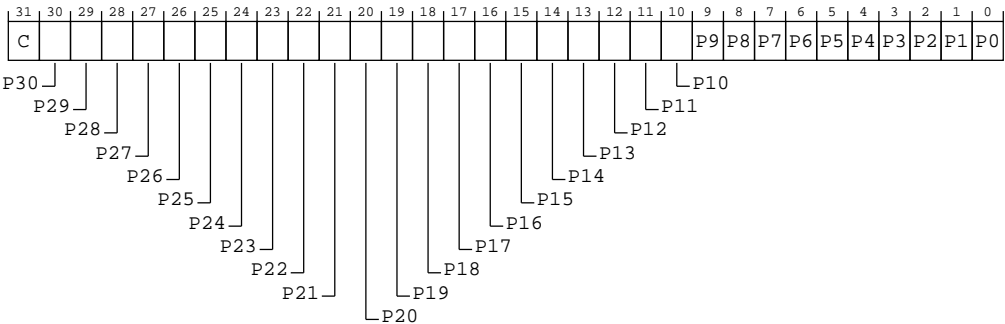


Table B-944: PMCNTENCLR\_ELO bit descriptions

Bits	Name	Description	Reset
[31]	C	PMU.PMCCNTR_ELO disable. On writes, allows software to disable PMU.PMCCNTR_ELO. On reads, returns the PMU.PMCCNTR_ELO enable status.  <b>0b0</b> PMU.PMCCNTR_ELO disabled.  <b>0b1</b> PMU.PMCCNTR_ELO enabled.  Access to this field is: W1C	x
[30:0]	P<m>, bit[m], where m = 30 to 0	PMEVCNTR<m>_ELO disable. On writes, allows software to disable PMEVCNTR<m>_ELO. On reads, returns the PMEVCNTR<m>_ELO enable status.  <b>0b0</b> PMEVCNTR<m>_ELO disabled.  <b>0b1</b> PMEVCNTR<m>_ELO enabled.  <b>When m &gt;= 6</b> Access to this field is: <b>RAZ/WI</b>  <b>Otherwise</b> Access to this field is: W1C	31 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xC20	PMCNTENCLR_ELO	31:0



B.2.2.8.11 PMINTENSET\_EL1, Performance Monitors Interrupt Enable Set Register

Enables the generation of interrupt requests on overflows from the Cycle Count Register, PMU.PMCCNTR\_EL0, and the event counters PMU.PMEVCNTR<n>\_EL0. Reading the register shows which overflow interrupt requests are enabled.

Configurations

PMINTENSET\_EL1 is in the Core power domain.

External register PMINTENSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.1 PMINTENSET\\_EL1, Performance Monitors Interrupt Enable Set Register](#) on page 752 bits [31:0].

External register PMINTENSET\_EL1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.2 PMINTENCLR\\_EL1, Performance Monitors Interrupt Enable Clear Register](#) on page 755 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xC40

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0

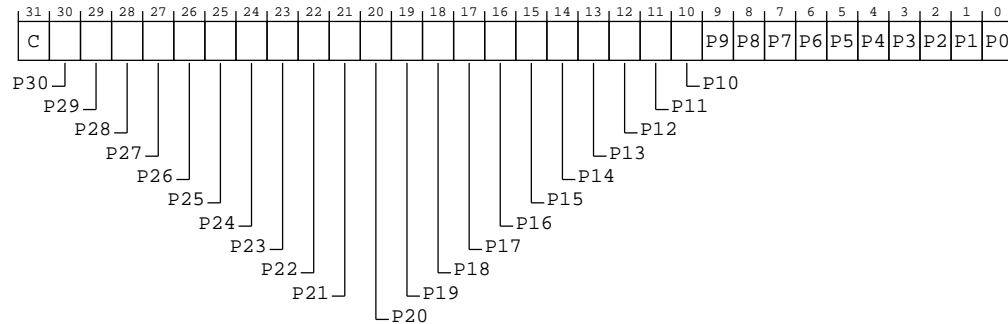


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-481: PMU\_PMINTENSET\_EL1 bit assignments**



**Table B-946: PMINTENSET\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31]	C	<p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO enable. On writes, allows software to enable the interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO. On reads, returns the interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO enabled.</p> <p>Access to this field is: W1S</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable. On writes, allows software to enable the interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO. On reads, returns the interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p><b>When m &gt;= 6</b></p> <p>Access to this field is: <b>RAZ/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: W1S</p>	31 {x}

## Accessibility

Component	Offset	Instance	Range
PMU	0xC40	PMINTENSET_EL1	31:0

B.2.2.8.12 PMINTENCLR\_EL1, Performance Monitors Interrupt Enable Clear Register

Disables the generation of interrupt requests on overflows from the Cycle Count Register, PMU.PMCCNTR\_ELO, and the event counters PMU.PMEVCNTR<n>\_ELO. Reading the register shows which overflow interrupt requests are enabled.

Configurations

PMINTENCLR\_EL1 is in the Core power domain.

External register PMINTENCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register A.2.3.2 PMINTENCLR\_EL1, Performance Monitors Interrupt Enable Clear Register on page 755 bits [31:0].

External register PMINTENCLR\_EL1 bits [31:0] are architecturally mapped to AArch64 System register A.2.3.1 PMINTENSET\_EL1, Performance Monitors Interrupt Enable Set Register on page 752 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xC60

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0

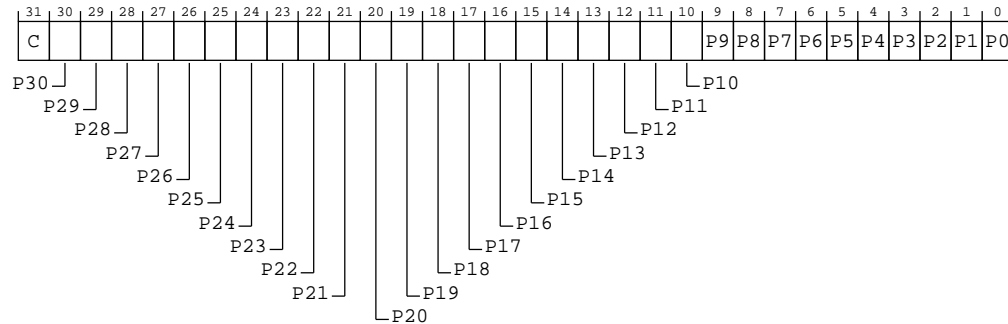


Note

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-482: PMU\_PMINTENCLR\_EL1 bit assignments**



**Table B-948: PMINTENCLR\_EL1 bit descriptions**

Bits	Name	Description	Reset
[31]	C	<p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO disable. On writes, allows software to disable the interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO. On reads, returns the interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMU.PMCCNTR_ELO enabled.</p> <p>Access to this field is: W1C</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disable. On writes, allows software to disable the interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO. On reads, returns the interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enable status.</p> <p><b>0b0</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO disabled.</p> <p><b>0b1</b></p> <p>Interrupt request or PMU exception on unsigned overflow of PMEVCNTR&lt;m&gt;_ELO enabled.</p> <p><b>When m &gt;= 6</b></p> <p>Access to this field is: <b>RAZ/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: W1C</p>	31 {x}

## Accessibility

Component	Offset	Instance	Range
PMU	0xC60	PMINTENCLR_EL1	31:0

B.2.2.8.13 PMOVSCLR\_ELO, Performance Monitors Overflow Flag Status Clear register

Contains the state of the overflow bit for the Cycle Count Register, PMU.PMCCNTR\_ELO, and each of the implemented event counters AArch32-PMEVCNTR<n>. Writing to this register clears these bits.

Configurations

PMOVSCLR\_ELO is in the Core power domain.

External register PMOVSCLR\_ELO bits [31:0] are architecturally mapped to AArch64 System register A.2.3.22 PMOVSCLR\_ELO, Performance Monitors Overflow Flag Status Clear Register on page 810 bits [31:0].

External register PMOVSCLR\_ELO bits [31:0] are architecturally mapped to AArch64 System register A.2.3.31 PMOVSSET\_ELO, Performance Monitors Overflow Flag Status Set Register on page 845 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xC80

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-483: PMU\_PMOVSLR\_ELO bit assignments

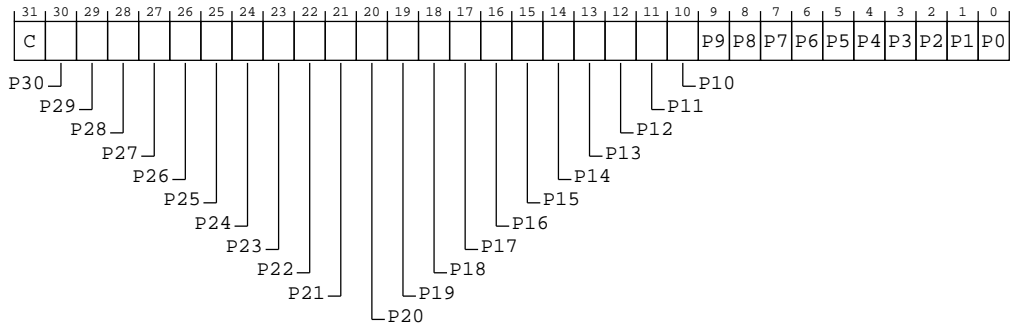


Table B-950: PMOVSLR\_ELO bit descriptions

Bits	Name	Description	Reset
[31]	C	Unsigned overflow flag for PMU.PMCCNTR_ELO clear. On writes, allows software to clear the unsigned overflow flag for PMU.PMCCNTR_ELO to 0. On reads, returns the unsigned overflow flag for PMU.PMCCNTR_ELO overflow status.  <b>0b0</b> PMU.PMCCNTR_ELO has not overflowed.  <b>0b1</b> PMU.PMCCNTR_ELO has overflowed.  Access to this field is: W1C	x
[30:0]	P<m>, bit[m], where m = 30 to 0	Unsigned overflow flag for PMU.PMEVCNTR<m>_ELO clear. On writes, allows software to clear the unsigned overflow flag for PMU.PMEVCNTR<m>_ELO to 0. On reads, returns the unsigned overflow flag for PMU.PMEVCNTR<m>_ELO overflow status.  <b>0b0</b> PMU.PMEVCNTR<m>_ELO has not overflowed.  <b>0b1</b> PMU.PMEVCNTR<m>_ELO has overflowed.  <b>When m &gt;= 6</b> Access to this field is: <b>RAZ/WI</b>  <b>Otherwise</b> Access to this field is: W1C	31 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xC80	PMOVSLR_ELO	31:0

B.2.2.8.14 PMSWINC\_ELO, Performance Monitors Software Increment Register

Increments a counter that is configured to count the Software increment event, event 0x00. For more information, see SW\_INCR in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

Use of this register is deprecated.

External register PMSWINC\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.23 PMSWINC\\_ELO, Performance Monitors Software Increment Register](#) on page 813 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xCA0

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3
							0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-484: PMU\_PMSWINC\_ELO bit assignments

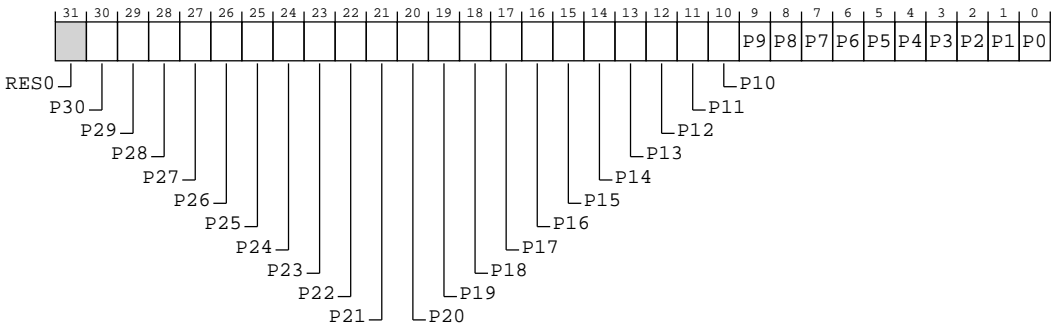


Table B-952: PMSWINC\_ELO bit descriptions

Bits	Name	Description	Reset
[31]	RES0	Reserved	RES0
[30:0]	P<n>, bit[n], where n = 30 to 0	Event counter software increment bit for PMU.PMEVCNTR<n>_ELO.  If PMU.PMCFGR.N is less than 31, bits [30:PMU.PMCFGR.N] are <b>wI</b> .  <b>0b0</b> No action. The write to this bit is ignored.  <b>0b1</b> A SW_INCR event is generated for event counter n.	31 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xCA0	PMSWINC_ELO	None

B.2.2.8.15 PMOVSET\_ELO, Performance Monitors Overflow Flag Status Set Register

Sets the state of the overflow bit for the Cycle Count Register, PMU.PMCCNTR\_ELO, and each of the implemented event counters PMU.PMEVCNTR<n>\_ELO.

Configurations

PMOVSET\_ELO is in the Core power domain.

External register PMOVSET\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.31 PMOVSET\\_ELO, Performance Monitors Overflow Flag Status Set Register](#) on page 845 bits [31:0].

External register PMOVSET\_ELO bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.22 PMOVCLR\\_ELO, Performance Monitors Overflow Flag Status Clear Register](#) on page 810 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

0xCC0

Reset value

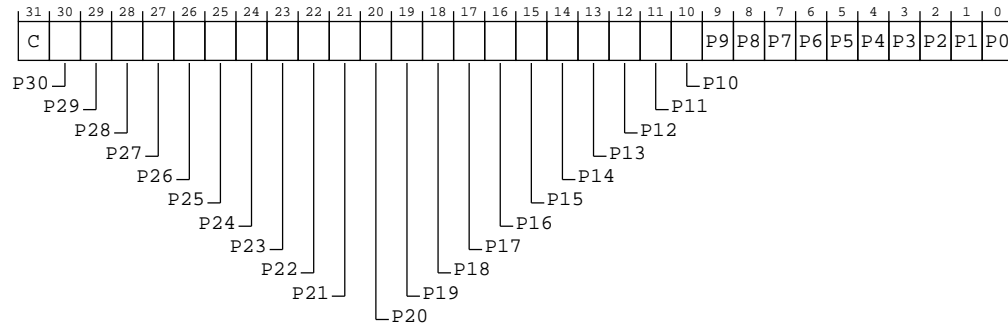




**Note**

Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-485: PMU\_PMOVSSET\_ELO bit assignments****Table B-954: PMOVSSET\_ELO bit descriptions**

Bits	Name	Description	Reset
[31]	C	<p>Unsigned overflow flag for PMU.PMCCNTR_ELO set. On writes, allows software to set the unsigned overflow flag for PMU.PMCCNTR_ELO to 1. On reads, returns the unsigned overflow flag for PMU.PMCCNTR_ELO overflow status.</p> <p><b>0b0</b></p> <p>PMU.PMCCNTR_ELO has not overflowed.</p> <p><b>0b1</b></p> <p>PMU.PMCCNTR_ELO has overflowed.</p> <p>Access to this field is: W1S</p>	x
[30:0]	P<m>, bit[m], where m = 30 to 0	<p>Unsigned overflow flag for PMU.PMEVCNTR&lt;m&gt;_ELO set. On writes, allows software to set the unsigned overflow flag for PMU.PMEVCNTR&lt;m&gt;_ELO to 1. On reads, returns the unsigned overflow flag for PMU.PMEVCNTR&lt;m&gt;_ELO overflow status.</p> <p><b>0b0</b></p> <p>PMU.PMEVCNTR&lt;m&gt;_ELO has not overflowed.</p> <p><b>0b1</b></p> <p>PMU.PMEVCNTR&lt;m&gt;_ELO has overflowed.</p> <p><b>When m &gt;= 6</b></p> <p>Access to this field is: <b>RAZ/WI</b></p> <p><b>Otherwise</b></p> <p>Access to this field is: W1S</p>	31 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xCC0	PMOVSSET_ELO	31:0

B.2.2.8.16 PMCFGR, Performance Monitors Configuration Register

Contains PMU-specific configuration data.

Configurations

PMCFGR is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xE00

Reset value

0000	xxxx	xxxx	0001	0111	1111	0000	0110
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-486: PMU\_PMCFG bit assignments

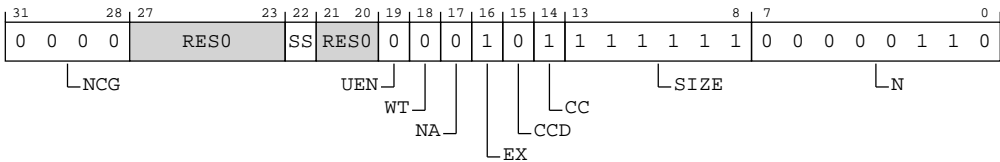


Table B-956: PMCFGR bit descriptions

Bits	Name	Description	Reset
[31:28]	NCG	Defines the number of counter groups implemented, minus one.  This field reads-as-zero. <b>0b0000</b>	0b0000
[27:23]	RES0	Reserved	RES0
[22]	SS	Snapshot supported. <b>0b0</b> Snapshot mechanism not supported. The locations 0x600-0x7FC and 0xE30-0xE3C are <b>IMPLEMENTATION DEFINED</b> . <b>0b1</b> Snapshot mechanism supported.  Locations 0x600-0x7FC and 0xE30-0xE3C contain <b>IMPLEMENTATION DEFINED</b> snapshot registers.  If the architecture-defined form of snapshot is not implemented, a PMU might include an <b>IMPLEMENTATION DEFINED</b> snapshot mechanism, including one using the <b>IMPLEMENTATION DEFINED</b> registers 0x600-0x7FC and 0xE30-0xE3C.	The reset values can be the following: 0b0, 0b1, respective to the value.
[21:20]	RES0	Reserved	RES0
[19]	UEN	User-mode Enable Register supported. AArch64-PMUSERENR_ELO is not visible in the external debug interface, so this bit is <b>RAZ</b> . <b>0b0</b>	0b0
[18]	WT	This feature is not supported, so this bit is <b>RAZ</b> . <b>0b0</b>	0b0
[17]	NA	This feature is not supported, so this bit is <b>RAZ</b> . <b>0b0</b>	0b0
[16]	EX	Export supported. Value is <b>IMPLEMENTATION DEFINED</b> . <b>0b1</b> PMU.PMCR_ELO.X is read/write.	0b1
[15]	CCD	Cycle counter has prescale.  This field is <b>RAZ</b> <b>0b0</b> PMU.PMCR_ELO.D is <b>RES0</b> .	0b0
[14]	CC	Dedicated cycle counter (counter 31) supported. <b>0b1</b>	0b1

Bits	Name	Description	Reset
[13:8]	SIZE	Size of counters, minus one. This field defines the size of the largest counter implemented by the Performance Monitors Unit.  From Armv8, the largest counter is 64-bits, so the value of this field is 0b111111.  This field is used by software to determine the spacing of the counters in the memory-map. From Armv8, the counters are a doubleword-aligned addresses. <b>0b111111</b>	0b111111
[7:0]	N	Number of counters implemented in addition to the cycle counter, ext-PMCCNTR_ELO. <b>0b00000110</b> ext-PMCCNTR_ELO plus 6 event counters implemented.	0x06

### Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

### Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Instance	Range
PMU	0xE00	PMCFGR	31:0

#### B.2.2.8.17 PMCR\_ELO, Performance Monitors Control Register

Provides details of the Performance Monitors implementation, including the number of counters implemented, and configures and controls the counters.

### Configurations

PMCR\_ELO is in the Core power domain.

External register PMCR\_ELO bits [63:32, 10:0] are architecturally mapped to AArch64 System register [A.2.3.19 PMCR\\_ELO, Performance Monitors Control Register](#) on page 801 bits [63:32].

### Attributes

#### Width

32

#### Component

PMU

#### Register offset

0xE04

#### Reset value

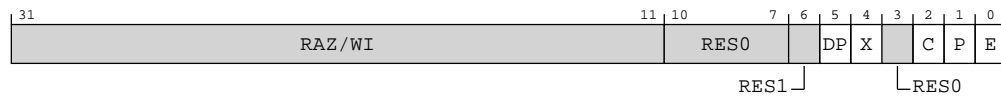
0000 0000 0000 0000 0000 0xxx xxx0 x000



Where the reset reads xxxx, see individual bits.

## Bit descriptions

**Figure B-487: PMU\_PMCR\_ELO bit assignments**



**Table B-958: PMCR\_ELO bit descriptions**

Bits	Name	Description	Reset
[31:11]	RAZ/WI	Reserved	RAZ/WI
[10:7]	RES0	Reserved	RES0
[6]	RES1	Reserved	RES1
[5]	DP	<p>Disable cycle counter when event counting is prohibited. The possible values of this bit are:</p> <p><b>0b0</b></p> <p>Cycle counting by PMU.PMCCNTR_ELO is not affected by this mechanism.</p> <p><b>0b1</b></p> <p>Cycle counting by PMU.PMCCNTR_ELO is disabled in prohibited regions and when event counting is frozen:</p> <ul style="list-style-type: none"> <li>If FEAT_PMUv3p1 is implemented, EL2 is implemented, and AArch64-MDCR_EL2.HPMD is 1, then cycle counting by PMU.PMCCNTR_ELO is disabled at EL2.</li> </ul> <p>If AArch64-MDCR_EL2.HPMN is not 0, this is when event counting by event counters in the range [0..(AArch64-MDCR_EL2.HPMN-1)] is prohibited or frozen.</p> <p>For more information, see <i>Prohibiting event and cycle counting</i> in the <a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>.</p>	x
[4]	X	<p>Enable export of events to the core trace unit (ETM).</p> <p><b>0b0</b></p> <p>Do not export events.</p> <p><b>0b1</b></p> <p>Export events to the ETM, where not prohibited.</p>	0b0
[3]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[2]	C	<p>Cycle counter reset. The effects of writing to this bit are:</p> <p><b>0b0</b></p> <p>No action.</p> <p><b>0b1</b></p> <p>Reset PMU.PMCCNTR_ELO to zero.</p> <p>Resetting PMU.PMCCNTR_ELO does not change the cycle counter overflow bit.</p> <p>Access to this field is: WO/<b>RAZ</b></p>	0b0
[1]	P	<p>Event counter reset. The effects of writing to this bit are:</p> <p><b>0b0</b></p> <p>No action.</p> <p><b>0b1</b></p> <p>Reset all event counters, not including PMU.PMCCNTR_ELO, to zero.</p> <p>Resetting the event counters does not change the event counter overflow bits.</p> <p>Access to this field is: WO/<b>RAZ</b></p>	0b0
[0]	E	<p>Enable.</p> <p>In the description of this field:</p> <ul style="list-style-type: none"> <li>If EL2 is implemented and is using AArch64, PMN is AArch64-MDCR_EL2.HPMN.</li> </ul> <p><b>0b0</b></p> <p>PMU.PMCCNTR_ELO is disabled and event counters PMU.PMEVCNTR&lt;n&gt;_ELO, where n is in the range of affected event counters, are disabled.</p> <p><b>0b1</b></p> <p>PMU.PMCCNTR_ELO and event counters PMU.PMEVCNTR&lt;n&gt;_ELO, where n is in the range of affected event counters, are enabled by PMU.PMCNTENSET_ELO.</p> <p>If PMN is not 0, this field affects the operation of event counters in the range [0 .. (PMN-1)].</p> <p>This field does not affect the operation of other event counters.</p>	0b0

### Accessibility

Component	Offset	Instance	Range
PMU	0xE04	PMCR_ELO	None

#### B.2.2.8.18 PMCEID0, Performance Monitors Common Event Identification register 0

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the range 0x0000 to 0x001F.

For more information about the Common events and the use of the PMCEIDn registers, see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).



This view of the register was previously called PMCEID0\_ELO.

Configurations

PMCEID0 is in the Core power domain.

External register PMCEID0 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.25 PMCEID0\\_ELO, Performance Monitors Common Event Identification Register 0](#) on page 817 bits [31:0].

Attributes

Width

32

Component

PMU

Register offset

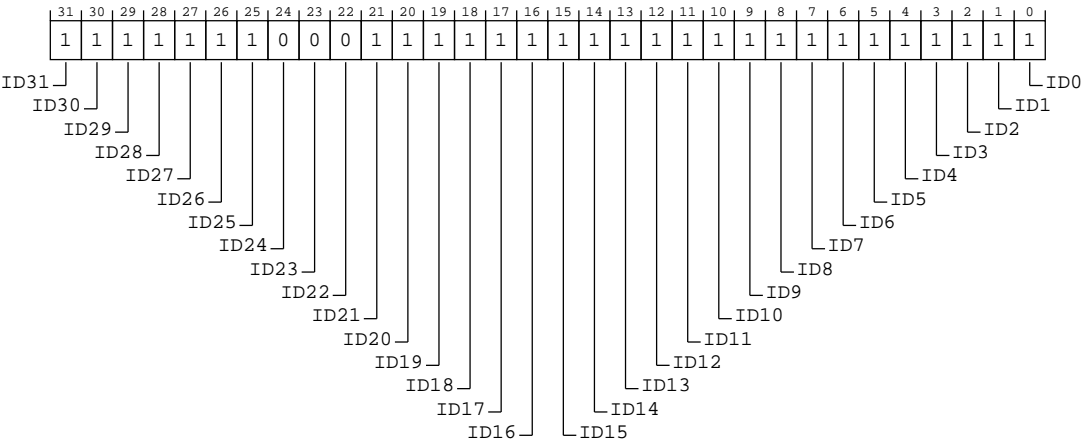
0xE20

Reset value

1111 1110 0011 1111 1111 1111 1111 1111

Bit descriptions

Figure B-488: PMU\_PMCEID0 bit assignments



**Table B-960: PMCEID0 bit descriptions**

Bits	Name	Description	Reset
[31]	ID31	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_ALLOCATE event implemented.	0b1
[30]	ID30	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CHAIN event implemented.	0b1
[29]	ID29	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BUS_CYCLES event implemented.	0b1
[28]	ID28	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> TTBR_WRITE_RETIRED event implemented.	0b1
[27]	ID27	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> INST_SPEC event implemented.	0b1
[26]	ID26	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> MEMORY_ERROR event implemented.	0b1
[25]	ID25	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BUS_ACCESS event implemented.	0b1
[24]	ID24	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0018 not implemented.	0b0
[23]	ID23	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0017 not implemented.	0b0



Bits	Name	Description	Reset
[22]	ID22	ID[n] corresponds to Common event n.  For each bit: <b>0b0</b> Event 0x0016 not implemented.	0b0
[21]	ID21	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_WB event implemented.	0b1
[20]	ID20	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_CACHE event implemented.	0b1
[19]	ID19	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> MEM_ACCESS event implemented.	0b1
[18]	ID18	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_PRED event implemented.	0b1
[17]	ID17	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CPU_CYCLES event implemented.	0b1
[16]	ID16	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_MIS_PRED event implemented.	0b1
[15]	ID15	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> UNALIGNED_LDST_RETIRED event implemented.	0b1
[14]	ID14	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_RETURN_RETIRED event implemented.	0b1

Bits	Name	Description	Reset
[13]	ID13	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> BR_IMMED_RETIRED event implemented.	0b1
[12]	ID12	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> PC_WRITE_RETIRED event implemented.	0b1
[11]	ID11	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> CID_WRITE_RETIRED event implemented.	0b1
[10]	ID10	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> EXC_RETURN event implemented.	0b1
[9]	ID9	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> EXC_TAKEN event implemented.	0b1
[8]	ID8	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> INST_RETIRED event implemented.	0b1
[7]	ID7	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> ST_RETIRED event implemented.	0b1
[6]	ID6	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> LD_RETIRED event implemented.	0b1
[5]	ID5	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_TLB_REFILL event implemented.	0b1

Bits	Name	Description	Reset
[4]	ID4	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE event implemented.	0b1
[3]	ID3	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1D_CACHE_REFILL event implemented.	0b1
[2]	ID2	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_TLB_REFILL event implemented.	0b1
[1]	ID1	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> L1I_CACHE_REFILL event implemented.	0b1
[0]	ID0	ID[n] corresponds to Common event n.  For each bit: <b>0b1</b> SW_INCR event implemented.	0b1

### Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

### Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Instance	Range
PMU	0xE20	PMCEID0	None

#### B.2.2.8.19 PMCEID1, Performance Monitors Common Event Identification register 1

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the range 0x020 to 0x03F.

For more information about the Common events and the use of the PMCEIDn registers, see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).



This view of the register was previously called PMCEID1\_EL0.

## Configurations

PMCEID1 is in the Core power domain.

External register PMCEID1 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.26 PMCEID1\\_EL0, Performance Monitors Common Event Identification Register 1](#) on page 826 bits [31:0].

## Attributes

### Width

32

### Component

PMU

### Register offset

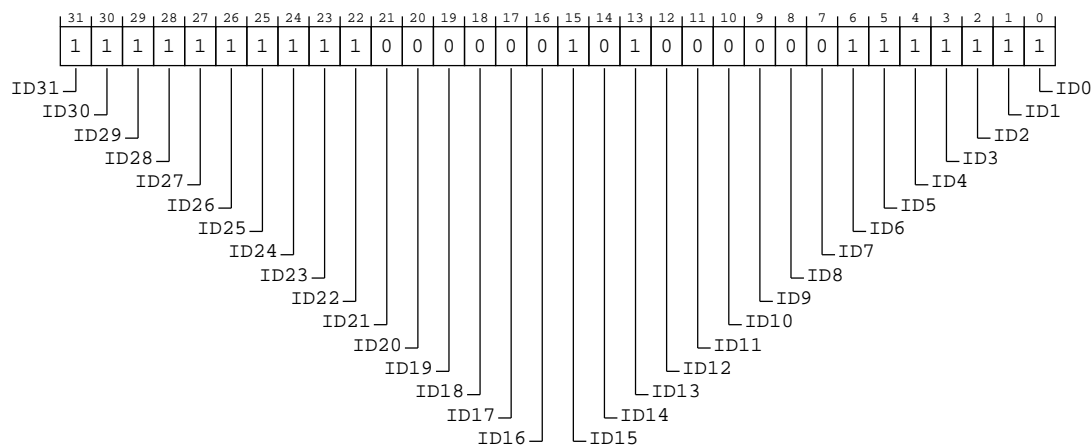
0xE24

### Reset value

1111 1111 1100 0000 1010 0000 0111 1111

## Bit descriptions

**Figure B-489: PMU\_PMCEID1 bit assignments**



**Table B-962: PMCEID1 bit descriptions**

Bits	Name	Description	Reset
[31]	ID31	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT event implemented.	0b1
[30]	ID30	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT_FRONTEND event implemented.	0b1
[29]	ID29	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_SLOT_BACKEND event implemented.	0b1
[28]	ID28	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL event implemented.	0b1
[27]	ID27	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> OP_SPEC event implemented.	0b1
[26]	ID26	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> OP_RETIRED event implemented.	0b1
[25]	ID25	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1D_CACHE_LMISS_RD event implemented.	0b1
[24]	ID24	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> REMOTE_ACCESS_RD event implemented.	0b1
[23]	ID23	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> LL_CACHE_MISS_RD event implemented.	0b1

Bits	Name	Description	Reset
[22]	ID22	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> LL_CACHE_RD event implemented.	0b1
[21]	ID21	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0035 not implemented.	0b0
[20]	ID20	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0034 not implemented.	0b0
[19]	ID19	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0033 not implemented.	0b0
[18]	ID18	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0032 not implemented.	0b0
[17]	ID17	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0031 not implemented.	0b0
[16]	ID16	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0030 not implemented.	0b0
[15]	ID15	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_TLB event implemented.	0b1
[14]	ID14	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002E not implemented.	0b0

Bits	Name	Description	Reset
[13]	ID13	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_TLB_REFILL event implemented.	0b1
[12]	ID12	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002C not implemented.	0b0
[11]	ID11	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002B not implemented.	0b0
[10]	ID10	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x002A not implemented.	0b0
[9]	ID9	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0029 not implemented.	0b0
[8]	ID8	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0028 not implemented.	0b0
[7]	ID7	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b0</b> Event 0x0027 not implemented.	0b0
[6]	ID6	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1I_TLB event implemented.	0b1
[5]	ID5	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L1D_TLB event implemented.	0b1

Bits	Name	Description	Reset
[4]	ID4	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_BACKEND event implemented.	0b1
[3]	ID3	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> STALL_FRONTEND event implemented.	0b1
[2]	ID2	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> BR_MIS_PRED_RETIRED event implemented.	0b1
[1]	ID1	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> BR_RETIRED event implemented.	0b1
[0]	ID0	ID[n] corresponds to Common event (0x0020 + n).  For each bit: <b>0b1</b> L2D_CACHE_ALLOCATE event implemented.	0b1

### Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

### Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Instance	Range
PMU	0xE24	PMCEID1	None

#### B.2.2.8.20 PMCEID2, Performance Monitors Common Event Identification register 2

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the range 0x4000 to 0x401F.

For more information about the Common events and the use of the PMCEIDn registers, see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).



Configurations

PMCEID2 is in the Core power domain.

External register PMCEID2 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.25 PMCEID0\\_EL0, Performance Monitors Common Event Identification Register 0](#) on page 817 bits [63:32].

Attributes

Width

32

Component

PMU

Register offset

0xE28

Reset value

0000 0000 0000 0000 0000 0000 0100 0000

Bit descriptions

Figure B-490: PMU\_PMCEID2 bit assignments

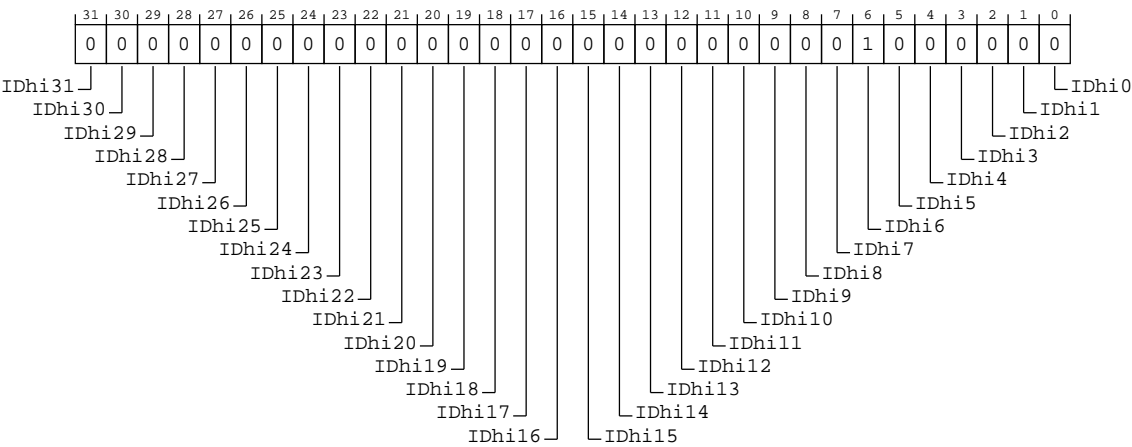


Table B-964: PMCEID2 bit descriptions

Bits	Name	Description	Reset
[31]	IDHi31	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b>  Event 0x401F not implemented.	0b0

Bits	Name	Description	Reset
[30]	IDHi30	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401E not implemented.	0b0
[29]	IDHi29	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401D not implemented.	0b0
[28]	IDHi28	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401C not implemented.	0b0
[27]	IDHi27	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401B not implemented.	0b0
[26]	IDHi26	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x401A not implemented.	0b0
[25]	IDHi25	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4019 not implemented.	0b0
[24]	IDHi24	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4018 not implemented.	0b0
[23]	IDHi23	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4017 not implemented.	0b0
[22]	IDHi22	IDHi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4016 not implemented.	0b0

Bits	Name	Description	Reset
[21]	IDhi21	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4015 not implemented.	0b0
[20]	IDhi20	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4014 not implemented.	0b0
[19]	IDhi19	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4013 not implemented.	0b0
[18]	IDhi18	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4012 not implemented.	0b0
[17]	IDhi17	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4011 not implemented.	0b0
[16]	IDhi16	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4010 not implemented.	0b0
[15]	IDhi15	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400F not implemented.	0b0
[14]	IDhi14	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400E not implemented.	0b0
[13]	IDhi13	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400D not implemented.	0b0

Bits	Name	Description	Reset
[12]	IDhi12	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400C not implemented.	0b0
[11]	IDhi11	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400B not implemented.	0b0
[10]	IDhi10	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x400A not implemented.	0b0
[9]	IDhi9	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4009 not implemented.	0b0
[8]	IDhi8	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4008 not implemented.	0b0
[7]	IDhi7	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4007 not implemented.	0b0
[6]	IDhi6	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b1</b> L1I_CACHE_LMISS event implemented.	0b1
[5]	IDhi5	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4005 not implemented.	0b0
[4]	IDhi4	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4004 not implemented.	0b0

Bits	Name	Description	Reset
[3]	IDhi3	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4003 not implemented.	0b0
[2]	IDhi2	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4002 not implemented.	0b0
[1]	IDhi1	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4001 not implemented.	0b0
[0]	IDhi0	IDhi[n] corresponds to Common event (0x4000 + n).  For each bit: <b>0b0</b> Event 0x4000 not implemented.	0b0

### Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

### Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Instance	Range
PMU	0xE28	PMCEID2	None

#### B.2.2.8.21 PMCEID3, Performance Monitors Common Event Identification register 3

Defines which Common architectural events and Common microarchitectural events are implemented, or counted, using PMU events in the range 0x4020 to 0x403F.

For more information about the Common events and the use of the PMCEIDn registers, see *The PMU event number space and common events* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Configurations

PMCEID3 is in the Core power domain.

External register PMCEID3 bits [31:0] are architecturally mapped to AArch64 System register [A.2.3.26 PMCEID1\\_EL0, Performance Monitors Common Event Identification Register 1](#) on page 826 bits [63:32].

Attributes

Width

32

Component

PMU

Register offset

0xE2C

Reset value

0000 0000 0000 0000 0000 0000 0000 0111

Bit descriptions

Figure B-491: PMU\_PMCEID3 bit assignments

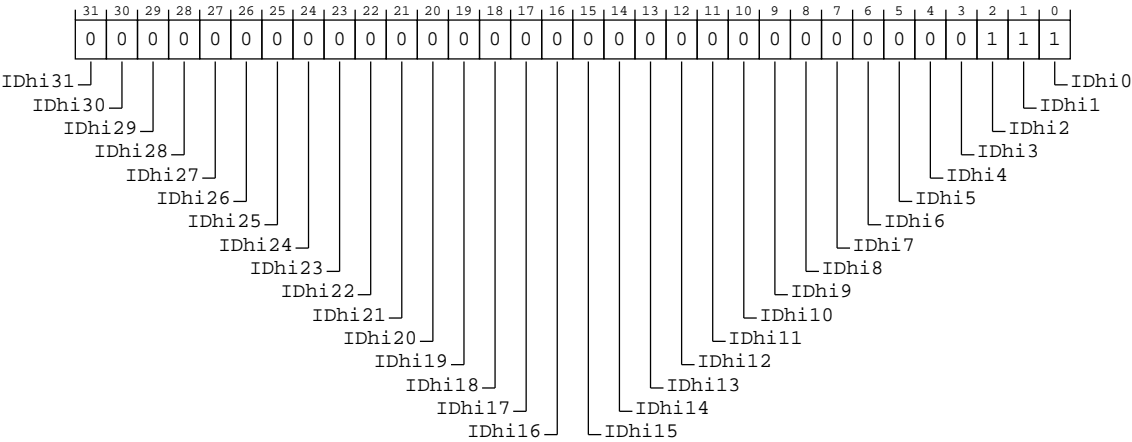


Table B-966: PMCEID3 bit descriptions

Bits	Name	Description	Reset
[31]	IDhi31	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403F not implemented.	0b0
[30]	IDhi30	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403E not implemented.	0b0

Bits	Name	Description	Reset
[29]	IDHi29	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403D not implemented.	0b0
[28]	IDHi28	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403C not implemented.	0b0
[27]	IDHi27	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403B not implemented.	0b0
[26]	IDHi26	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x403A not implemented.	0b0
[25]	IDHi25	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4039 not implemented.	0b0
[24]	IDHi24	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4038 not implemented.	0b0
[23]	IDHi23	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4037 not implemented.	0b0
[22]	IDHi22	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4036 not implemented.	0b0
[21]	IDHi21	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4035 not implemented.	0b0

Bits	Name	Description	Reset
[20]	IDHi20	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4034 not implemented.	0b0
[19]	IDHi19	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4033 not implemented.	0b0
[18]	IDHi18	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4032 not implemented.	0b0
[17]	IDHi17	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4031 not implemented.	0b0
[16]	IDHi16	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4030 not implemented.	0b0
[15]	IDHi15	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402F not implemented.	0b0
[14]	IDHi14	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402E not implemented.	0b0
[13]	IDHi13	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402D not implemented.	0b0
[12]	IDHi12	IDHi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402C not implemented.	0b0



Bits	Name	Description	Reset
[11]	IDhi11	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402B not implemented.	0b0
[10]	IDhi10	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x402A not implemented.	0b0
[9]	IDhi9	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4029 not implemented.	0b0
[8]	IDhi8	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4028 not implemented.	0b0
[7]	IDhi7	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4027 not implemented.	0b0
[6]	IDhi6	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4026 not implemented.	0b0
[5]	IDhi5	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4025 not implemented.	0b0
[4]	IDhi4	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4024 not implemented.	0b0
[3]	IDhi3	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b0</b> Event 0x4023 not implemented.	0b0

Bits	Name	Description	Reset
[2]	IDhi2	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> ST_ALIGN_LAT event implemented.	0b1
[1]	IDhi1	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> LD_ALIGN_LAT event implemented.	0b1
[0]	IDhi0	IDhi[n] corresponds to Common event (0x4020 + n).  For each bit: <b>0b1</b> LDST_ALIGN_LAT event implemented.	0b1

### Access

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

### Accessibility

AllowExternalPMUAccess() has a new definition from Armv8.4. Refer to the Pseudocode definitions for more information.

Component	Offset	Instance	Range
PMU	0xE2C	PMCEID3	None

#### B.2.2.8.22 PMMIR, Performance Monitors Machine Identification Register

Describes Performance Monitors parameters specific to the implementation.

### Configurations

PMMIR is in the Core power domain.

### Attributes

#### Width

32

#### Component

PMU

#### Register offset

0xE40

## Reset value

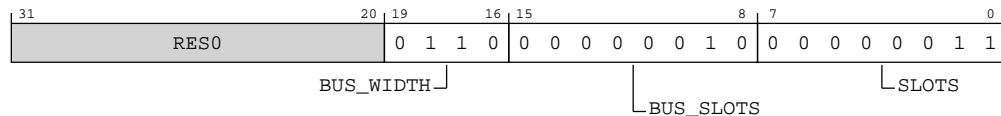
xxxx	xxxx	xxxx	0110	0000	0010	0000	0011
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

## Bit descriptions

### Figure B-492: PMU\_PMMIR bit assignments



### Table B-968: PMMIR bit descriptions

Bits	Name	Description	Reset
[31:20]	RES0	Reserved	RES0
[19:16]	BUS_WIDTH	<p>Bus width. Indicates the number of bytes each BUS_ACCESS event relates to. Encoded as <math>\text{Log}_2(\text{number of bytes})</math>, plus one.</p> <p><b>0b0110</b> 32 bytes.</p> <p>All other values are reserved.</p> <p>Each transfer is up to this number of bytes. An access might be smaller than the bus width.</p> <p>When this field is nonzero, each access counted by BUS_ACCESS is at most BUS_WIDTH bytes. An implementation might treat a wide bus as multiple narrower buses, such that a wide access on the bus increments the BUS_ACCESS counter by more than one.</p>	0b0110
[15:8]	BUS_SLOTS	<p>Bus count. The largest value by which the BUS_ACCESS event might increment in a single BUS_CYCLES cycle.</p> <p><b>0b00000010</b> The BUS_ACCESS event might increment by at most 2 in a single BUS_CYCLES cycle.</p> <p>When this field is nonzero, the largest value by which the BUS_ACCESS event might increment in a single BUS_CYCLES cycle is BUS_SLOTS.</p> <p>If the bus count information is not available, this field will read as zero.</p>	0x02
[7:0]	SLOTS	<p>Operation width. The largest value by which the STALL_SLOT event might increment in a single cycle.</p> <p><b>0b00000011</b> STALL_SLOT may increment by up to 3 in a single cycle.</p>	0x03

Accessibility

If the Core power domain is off or in a low-power state, access on this interface returns an Error.

Component	Offset	Instance	Range
PMU	0xE40	PMMIR	31:0

B.2.2.8.23 PMITCTRL, Performance Monitors Integration mode Control register

Enables the Performance Monitors to switch from default mode into integration mode, where test software can control directly the inputs and outputs of the PE, for integration testing or topology detection.

Configurations

This register is in the Core power domain.

Attributes

Width

32

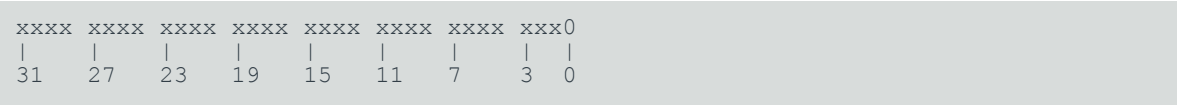
Component

PMU

Register offset

0xF00

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-493: PMU\_PMITCTRL bit assignments

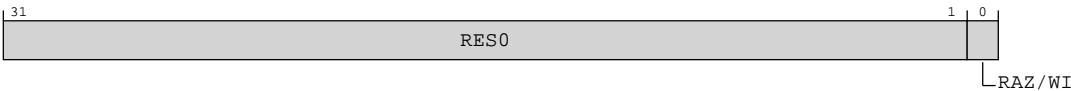


Table B-970: PMITCTRL bit descriptions

Bits	Name	Description	Reset
[31:1]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[0]	RAZ/WI	Reserved	RAZ/WI

Accessibility

Component	Offset	Instance	Range
PMU	0xF00	PMITCTRL	None

B.2.2.8.24 PMDEVAFF0, Performance Monitors Device Affinity register 0

Copy of the low half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the Performance Monitor component relates to.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFA8

Reset value



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-494: PMU\_PMDEVAFF0 bit assignments

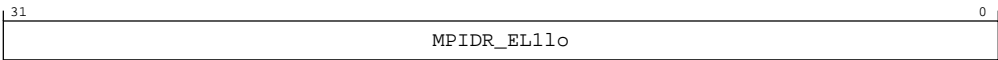


Table B-972: PMDEVAFF0 bit descriptions

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1lo	AArch64-MPIDR_EL1 low half. Read-only copy of the low half of AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.	32 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xFA8	PMDEVAFF0	None

B.2.2.8.25 PMDEVAFF1, Performance Monitors Device Affinity register 1

Copy of the high half of the PE AArch64-MPIDR\_EL1 register that allows a debugger to determine which PE in a multiprocessor system the Performance Monitor component relates to.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFAC

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-495: PMU\_PMDEVAFF1 bit assignments

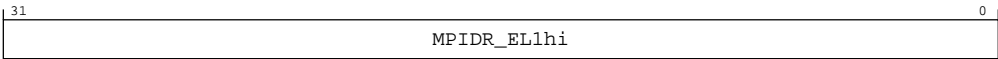


Table B-974: PMDEVAFF1 bit descriptions

Bits	Name	Description	Reset
[31:0]	MPIDR_EL1hi	AArch64-MPIDR_EL1 high half. Read-only copy of the high half of AArch64-MPIDR_EL1, as seen from the highest implemented Exception level.	32 {x}

Accessibility

Component	Offset	Instance	Range
PMU	0xFAC	PMDEVAFF1	None

B.2.2.8.26 PMLAR, Performance Monitors Lock Access Register

Allows or disallows access to the Performance Monitors registers through a memory-mapped interface.

The optional Software Lock provides a lock to prevent memory-mapped writes to the Performance Monitors registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the Performance Monitors registers. It does not, and cannot, prevent all accidental or malicious damage.

Configurations

Software Lock is not implemented by the architecturally-defined debug components of the PE in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFB0

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Otherwise

Figure B-496: PMU\_PMLAR bit assignments

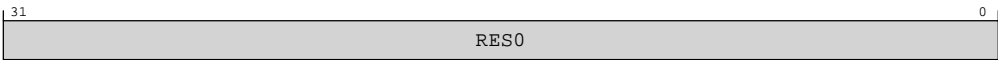


Table B-976: PMLAR bit descriptions

Bits	Name	Description	Reset
[31:0]	RES0	Reserved	RES0

Accessibility

Component	Offset	Instance	Range
PMU	0xFB0	PMLAR	None

B.2.2.8.27 PMLSR, Performance Monitors Lock Status Register

Indicates the current status of the software lock for Performance Monitors registers.

The optional Software Lock provides a lock to prevent memory-mapped writes to the Performance Monitors registers. Use of this lock mechanism reduces the risk of accidental damage to the contents of the Performance Monitors registers. It does not, and cannot, prevent all accidental or malicious damage.

Configurations

Software Lock is not implemented by the architecturally-defined debug components of the PE in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFB4

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	x000
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.



Bit descriptions

Figure B-497: PMU\_PMLSR bit assignments

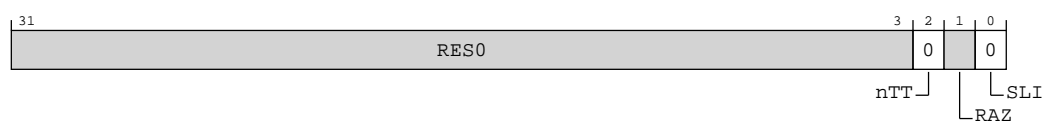


Table B-978: PMLSR bit descriptions

Bits	Name	Description	Reset
[31:3]	RES0	Reserved	RES0
[2]	nTT	Not thirty-two bit access required. 0b0	0b0
[1]	RAZ	Reserved	RAZ
[0]	SLI	Indicates whether the Software Lock is implemented. 0b0 Software Lock not implemented or not memory-mapped access.	0b0

Accessibility

Component	Offset	Instance	Range
PMU	0xFB4	PMLSR	None

B.2.2.8.28 PMAUTHSTATUS, Performance Monitors Authentication Status register

Provides information about the state of the **IMPLEMENTATION DEFINED** authentication interface for Performance Monitors.

Configurations

This register is in the Core power domain.

Attributes

Width

32

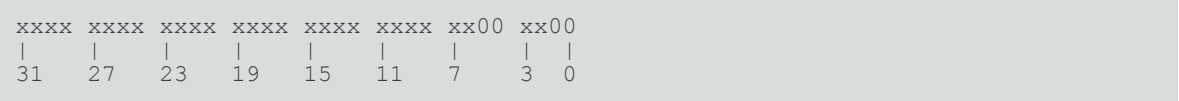
Component

PMU

Register offset

0xFB8

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-498: PMU\_PMAUTHSTATUS bit assignments

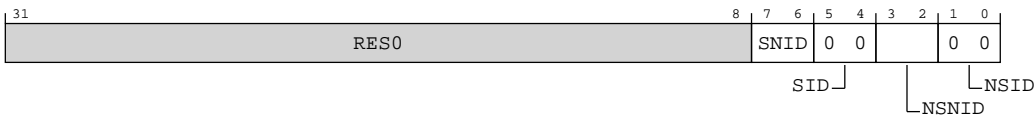


Table B-980: PMAUTHSTATUS bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:6]	SNID	Holds the same value as ext-DBGAUTHSTATUS_EL1.SNID.	xx
[5:4]	SID	Secure invasive debug. Possible values of this field are:  0b00 Not implemented.	0b00
[3:2]	NSNID	Holds the same value as ext-DBGAUTHSTATUS_EL1.NSNID.	xx
[1:0]	NSID	Non-secure invasive debug. Possible values of this field are:  0b00 Not implemented.	0b00

Accessibility

Component	Offset	Instance	Range
PMU	0xFB8	PMAUTHSTATUS	None

B.2.2.8.29 PMDEVARCH, Performance Monitors Device Architecture register

Identifies the programmers' model architecture of the Performance Monitor component.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFBC

Reset value

0100 0111 0111 0000 0010 1010 0001 0110

Bit descriptions

Figure B-499: PMU\_PMDEVARCH bit assignments

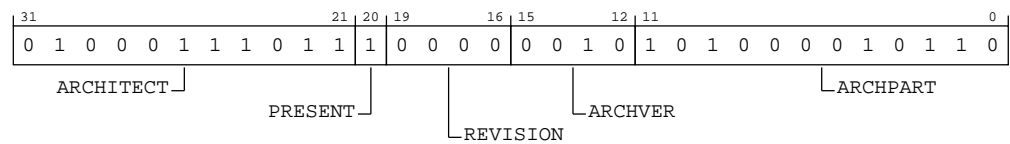


Table B-982: PMDEVARCH bit descriptions

Bits	Name	Description	Reset
[31:21]	ARCHITECT	Defines the architecture of the component. For Performance Monitors, this is Arm Limited.  Bits [31:28] are the JEP106 continuation code, 0x4.  Bits [27:21] are the JEP106 ID code, 0x3B. <b>0b01000111011</b>	0b01000111011
[20]	PRESENT	Indicates that the DEVARCH is present. <b>0b1</b>	0b1
[19:16]	REVISION	Defines the architecture revision. For architectures defined by Arm this is the minor revision.  For Performance Monitors, the revision defined by Armv8 is 0x0.  All other values are reserved. <b>0b0000</b>	0b0000
[15:12]	ARCHVER	Architecture Version. Defines the architecture version of the component. <b>0b0010</b> Performance Monitors Extension version 3, PMUv3.	0b0010
[11:0]	ARCHPART	Architecture Part. Defines the architecture of the component. <b>0b101000010110</b> Armv8-A PE performance monitors.  PMDEVARCH.ARCHVER and PMDEVARCH.ARCHPART are also defined as a single field, PMDEVARCH.ARCHID, so that PMDEVARCH.ARCHPART is PMDEVARCH.ARCHID[11:0].	0xA16

Accessibility

Component	Offset	Instance	Range
PMU	0xFBC	PMDEVARCH	None

B.2.2.8.30 PMDEVID, Performance Monitors Device ID register

Provides information about features of the Performance Monitors implementation.

Configurations

This register is in the Core power domain.

Attributes

Width

32

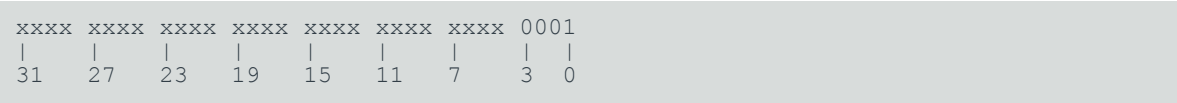
Component

PMU

Register offset

0xFC8

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-500: PMU\_PMDEVID bit assignments



Table B-984: PMDEVID bit descriptions

Bits	Name	Description	Reset
[31:4]	RES0	Reserved	RES0
[3:0]	PCSample	Indicates the level of PC Sample-based Profiling support using Performance Monitors registers.  0b0001 PC Sample-based Profiling Extension is implemented in the Performance Monitors register space.	0b0001

Accessibility

Component	Offset	Instance	Range
PMU	0xFC8	PMDEVID	None

B.2.2.8.31 PMDEVTYPE, Performance Monitors Device Type register

Indicates to a debugger that this component is part of a PE's performance monitor interface.

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFCC

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0110
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-501: PMU\_PMDEVTYPE bit assignments

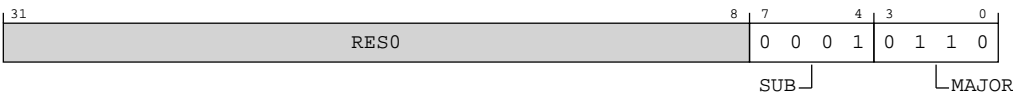


Table B-986: PMDEVTYPE bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	SUB	Subtype. Indicates this is a component within a PE. 0b0001	0b0001
[3:0]	MAJOR	Major type. Indicates this is a performance monitor component. 0b0110	0b0110

Accessibility

Component	Offset	Instance	Range
PMU	0xFCC	PMDEVTYPE	None

B.2.2.8.32 PMPIDR4, Performance Monitors Peripheral Identification Register 4

Provides information to identify a Performance Monitor component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFD0

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-502: PMU\_PMPIDR4 bit assignments

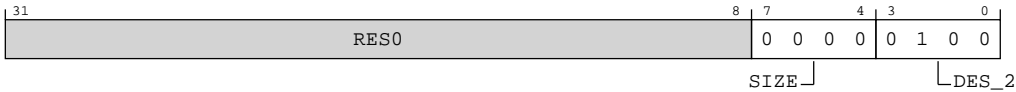


Table B-988: PMPIDR4 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	SIZE	Size of the component. <b>RAZ.</b> Log <sub>2</sub> of the number of 4KB pages from the start of the component to the end of the component ID registers.  <b>0b0000</b> The component uses a single 4KB block.	0b0000
[3:0]	DES_2	Designer, JEP106 continuation code, least significant nibble. For Arm Limited, this field is 0b0100.  <b>0b0100</b> Arm Limited. Number of 0x7F bytes in full JEP106 code 0x7F 0x7F 0x7F 0x7F 0x3B.	0b0100

Accessibility

Component	Offset	Instance	Range
PMU	0xFD0	PMPIDR4	None

B.2.2.8.33 PMPIDR0, Performance Monitors Peripheral Identification Register 0

Provides information to identify a Performance Monitor component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFE0

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0100
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-503: PMU\_PMPIDR0 bit assignments



Table B-990: PMPIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PART_0	Part number bits [7:0].  0b00010100 Cortex-R82AE PMU. Bits [7:0] of part number 0xD14.	0x14

Accessibility

Component	Offset	Instance	Range
PMU	0xFE0	PMPIDR0	None

B.2.2.8.34 PMPIDR1, Performance Monitors Peripheral Identification Register 1

Provides information to identify a Performance Monitor component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFE4

Reset value







Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-504: PMU\_PMPIDR1 bit assignments

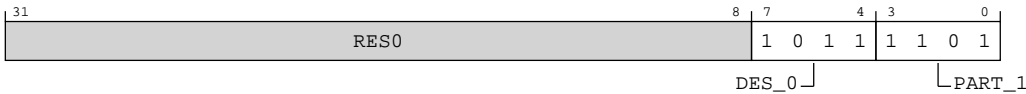


Table B-992: PMPIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	DES_0	Designer, least significant nibble of JEP106 ID code. For Arm Limited, this field is 0b1011.  0b1011 Arm Limited. Bits [3:0] of JEP106 identification code 0x3B.	0b1011
[3:0]	PART_1	Part number bits [11:8].  0b1101 Cortex-R82AE PMU. Bits [11:8] of part number 0xD14.	0b1101

Accessibility

Component	Offset	Instance	Range
PMU	0xFE4	PMPIDR1	None

B.2.2.8.35 PMPIDR2, Performance Monitors Peripheral Identification Register 2

Provides information to identify a Performance Monitor component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFE8

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-505: PMU\_PMPIDR2 bit assignments

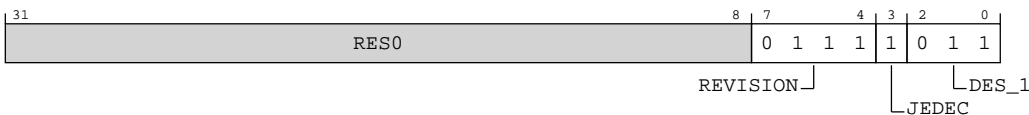


Table B-994: PMPIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVISION	Component revision.  0b0111 Revision 7.	0b0111
[3]	JEDEC	RAO. Indicates a JEP106 identity code is used.  0b1 JEDEC-assignee values is used.	0b1
[2:0]	DES_1	Designer, most significant bits of JEP106 ID code. For Arm Limited, this field is 0b011.  0b011 Arm Limited. Bits [6:4] of JEP106 identification code 0x3B.	0b011

Accessibility

Component	Offset	Instance	Range
PMU	0xFE8	PMPIDR2	None

B.2.2.8.36 PMPIDR3, Performance Monitors Peripheral Identification Register 3

Provides information to identify a Performance Monitor component.

For more information, see *About the Peripheral identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

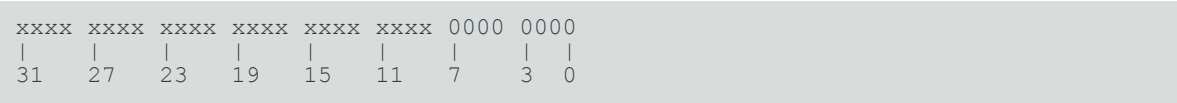
Component

PMU

Register offset

0xFEC

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-506: PMU\_PMPIDR3 bit assignments

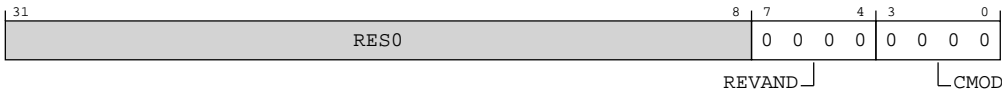


Table B-996: PMPIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:4]	REVAND	Part minor revision. Parts using ext-PMPIDR2.REVISION as an extension to the Part number must use this field as a major revision number.  0b0000 No ECO fixes.	0b0000
[3:0]	CMOD	Customer modified. Indicates someone other than the Designer has modified the component.  0b0000 The component is not modified from the original design.	0b0000

Accessibility

Component	Offset	Instance	Range
PMU	0xFEC	PMPIDR3	None

B.2.2.8.37 PMCIDR0, Performance Monitors Component Identification Register 0

Provides information to identify a Performance Monitor component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

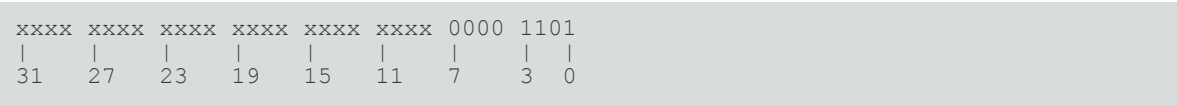
Component

PMU

Register offset

0xFF0

Reset value



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-507: PMU\_PMCIDR0 bit assignments

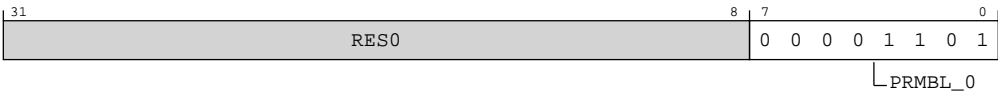


Table B-998: PMCIDR0 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_0	Preamble.  0b00001101 CoreSight component identification preamble.	0x0D

Accessibility

Component	Offset	Instance	Range
PMU	0xFF0	PMCIDR0	None

B.2.2.8.38 PMCIDR1, Performance Monitors Component Identification Register 1

Provides information to identify a Performance Monitor component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFF4

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	1001	0000
31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-508: PMU\_PMCIDR1 bit assignments

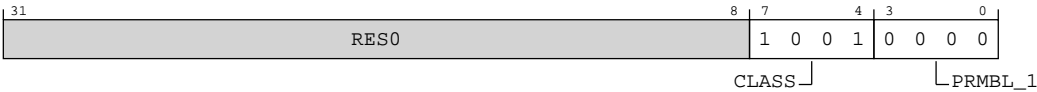


Table B-1000: PMCIDR1 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0

Bits	Name	Description	Reset
[7:4]	CLASS	Component class.  <b>0b1001</b> CoreSight debug component.	0b1001
[3:0]	PRMBL_1	Preamble.  <b>0b0000</b> CoreSight component identification preamble.	0b0000

Accessibility

Component	Offset	Instance	Range
PMU	0xFF4	PMCIDR1	None

B.2.2.8.39 PMCIDR2, Performance Monitors Component Identification Register 2

Provides information to identify a Performance Monitor component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

Component

PMU

Register offset

0xFF8

Reset value

xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	0000	0101
31	27	23	19	15	11	7	3 0



Note

Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-509: PMU\_PMCIDR2 bit assignments

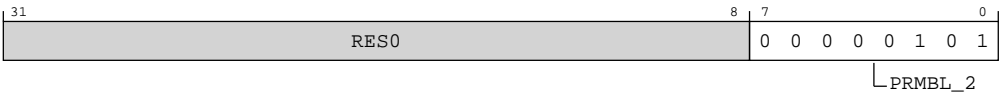


Table B-1002: PMCIDR2 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_2	Preamble.  0b00000101 CoreSight component identification preamble.	0x05

Accessibility

Component	Offset	Instance	Range
PMU	0xFF8	PMCIDR2	None

B.2.2.8.40 PMCIDR3, Performance Monitors Component Identification Register 3

Provides information to identify a Performance Monitor component.

For more information, see *About the Component Identification scheme* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is in the Core power domain.

Attributes

Width

32

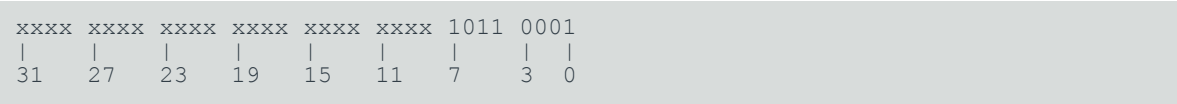
Component

PMU

Register offset

0xFFC

Reset value





Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure B-510: PMU\_PMCIDR3 bit assignments

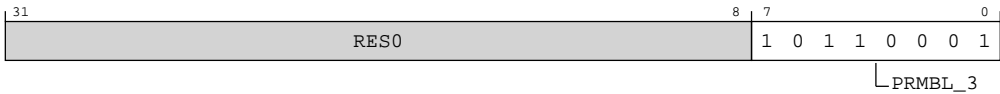


Table B-1004: PMCIDR3 bit descriptions

Bits	Name	Description	Reset
[31:8]	RES0	Reserved	RES0
[7:0]	PRMBL_3	Preamble.  0b10110001 CoreSight component identification preamble.	0xB1

Accessibility

Component	Offset	Instance	Range
PMU	0xFFC	PMCIDR3	None



# Appendix C Processor UNPREDICTABLE behaviors

This appendix describes the specific Cortex®-R82AE processor **UNPREDICTABLE** behaviors that differ from the Arm standard behavior.

For each case, the Arm standard specification is listed under *Specification* and the Cortex®-R82AE processor implementation is listed under *Implementation*. For detailed background information on **UNPREDICTABLE** behaviors, see [Arm® Architecture Reference Manual for A-profile architecture](#).

## C.1 SBZ or SBO fields in instructions

This section describes the specification and implementation of SBZ or SBO fields in instructions.

### Specification

Some instructions have (0) or (1) in the instruction decode to indicate *should-be-zero*, SBZ, or *should-be-one*, SBO. Except for specific cases identified in **CONSTRAINED UNPREDICTABLE** behaviors with Load-Exclusive/Store-Exclusive pairs as described in the [Arm® Architecture Reference Manual for A-profile architecture](#), if the instruction bit pattern of an instruction is executed with these fields not having the *should be* values, one of the following must occur:

- The instruction is **UNDEFINED**
- The instruction executes as a NOP
- The instruction operates as if the bit had the *should-be* value
- Any destination registers of the instruction become **UNKNOWN**
- For execution at EL0 or EL1, when EL2 is implemented and enabled for the current Security state and HCR\_EL2.TIDCP is 1, the instruction is trapped to EL2 with EC value 0

### Implementation

SBZ or SBO fields in instructions are treated as *don't care* conditions in the Cortex®-R82AE decoders. Therefore, the instructions execute as if the bit is 1 or 0 if it is an SBO or SBZ value irrespective of the actual bit value.

## C.2 CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values

This section describes the specification and implementation of caching of control or data values.

### Specification

The Arm architecture allows copies of control values or data values to be cached in a cache or TLB. This can lead to **UNPREDICTABLE** behavior if the cache or TLB has not been correctly invalidated following a change of the control or data values.

Unless explicitly stated otherwise, the behavior of the PE is consistent with one of:

- The old data or control value.
- The new data or control value.
- An amalgamation of the old and new data or control values.

The **CONSTRAINED UNPREDICTABLE** case can arise from misprogramming when setting TTBR.CnP to 1, as identified in the descriptions of the TTBR.CnP field. In this case, for a particular TTBR, the behavior of the PE is consistent with one of:

- The value of the translation table entry pointed to by that TTBR on one of the PEs within the Inner Shareable domain for which both the value of TTBR.CnP is 1 and the other conditions for sharing translation table entries pointed to by that TTBR are met.
- An amalgamation of the values of the translation table entries pointed to by that TTBR on two or more of the PEs within the Inner Shareable domain for which both the value of TTBR.CnP is 1 and the other conditions for sharing translation table entries pointed to by that TTBR are met.

### Implementation

For Cortex®-R82AE processor, copies of control values are not stored in a cache. For cached copies of data values, old data value will be returned unless the cache is invalidated either explicitly or by the coherency mechanism. Copies of control values can be cached in TLB. Therefore, if invalidation is not performed after updating the control values, an erroneous translation may occur.

Cortex®-R82AE processor does not store TTBR.CnP bit in the TLB as the Cortex®-R82AE processor does not use TTBR.CnP and the TLB is private to a core.

## C.3 CONSTRAINED UNPREDICTABLE behavior due to inadequate context synchronization

This section describes the specification and implementation of context synchronization.

### Specification

The Arm architecture requires that changes to System registers must be synchronized before they take effect. This can lead to **UNPREDICTABLE** behavior if the synchronization has not been performed. Where multiple control values are updated but not yet synchronized, each control value might independently be the old value or the new value.

### Implementation

For the Cortex®-R82AE processor, control bits in System registers that require explicit synchronization to reflect the updated value are listed below. All other System register control bits are updated immediately and do not require explicit context synchronization.

- SCTLR\_EL2 bits: EE, WXN, BR, I, NAA, C, A, M, SA, ENDA, ENDB, ENIA, ENIB
- SCTLR\_EL1 bits: EE, WXN, EOE, BR, I, NAA, SA0, SA, C, A, M, ENDA, ENDB, ENIA, ENIB
- IMP\_ITCMREGIONR\_EL1 bits: EL2, EL10
- IMP\_DTCMREGIONR\_EL1 bits: EL2, EL10
- IMP\_LLPPREGIONR\_EL1 bits: EL2, EL10
- IMP\_SPPREGIONR\_EL1 bits: EL2, EL10
- IMP\_LLDRAMREGIONR\_EL1 bits: EL2, EL10
- IMP\_MEMPROTCTLR\_EL1 bit: MEMPROTEN
- HCR\_EL2 bits: AMO, FMO, PTW, IMO, TGE, ID, DC, CD, VM, FWB, HCD
- CPACR\_EL1 bits: All
- CPTR\_EL2 bits: All
- CPUACTLR\_EL1 bits: IALLOC and IMCWT
- DBGAUTHSTATUS\_EL1 bits: DBGEN, SPIDEN
- EDSCR bits: HDE, TDA, TFO, INTdis
- OSLSR\_EL1 bits: OSLK

## C.4 Translation table base address alignment

This section describes the specification and implementation of translation table base address alignment.

### Specification

In the translation table base registers TTBRO\_EL1, TTBR1\_EL1, register bits[48:x] hold the translation table base address, where x depends on the translation table granule size and the

size of the addressed translation table. Register bits[(x-1):0], correspond to bits[(x-1):0] of the translation table base address and therefore are RES0.

For these registers, if one or more RES0 bits in register bits [(x-1):0] does not have a value of 0, this can result in a misaligned translation table base address. In this case, one of the following behaviors must occur:

- The field that is defined to be RES0 is treated as if all the bits had a value of 0:
  - The value read back might be the value written or it might be zero.
- The calculation of an address for a translation table walk using those registers might be corrupted in those bits that are nonzero.

### Implementation

For Cortex®-R82AE processor, if one or more RES0 bits in register bits [(x-1):0] does not have a value of 0, the field that is defined to be RES0 is treated as if all the bits had a value of 0 and the value read back is the value written.

## C.5 The Performance Monitors Extension

This section describes the specification and implementation of accessing the Performance Monitors Extension.

### C.5.1 CONSTRAINED UNPREDICTABLE accesses to PMXEVTYPER\_ELO or PMXEVCNTR\_ELO

This section describes the specification and implementation of accessing to PMXEVTYPER\_ELO or PMXEVCNTR\_ELO.

#### Specification

If PMSELR\_ELO.SEL is greater than the number of event counters accessible at this Exception level, accesses to PMXEVTYPER\_ELO and PMXEVCNTR\_ELO can cause **CONSTRAINED UNPREDICTABLE** behavior.

#### Implementation

In the Cortex®-R82AE processor, accesses to PMXEVTYPER\_ELO or PMXEVCNTR\_ELO from that state behave as RAZ/WI.

## C.5.2 CONSTRAINED UNPREDICTABLE accesses to PMEVCNTR<n>\_ELO and PMEVTYPER<n>\_ELO

This section describes the specification and implementation of accessing to PMEVCNTR<n>\_ELO and PMEVTYPER<n>\_ELO.

### Specification

If <n> is greater than the number of counters available in the current Exception level and state, reads and writes of PMEVCNTR<n>\_ELO and PMEVTYPER<n>\_ELO are **CONSTRAINED UNPREDICTABLE**.

### Implementation

For the Cortex®-R82AE processor, <n> is between 0-5 and accesses to the register are **UNDEFINED** when <n> is greater than 5.

## C.5.3 CONSTRAINED UNPREDICTABLE behavior caused by MDCR\_EL2.HPMN

This section describes the specification and implementation of **CONSTRAINED UNPREDICTABLE** behavior caused by MDCR\_EL2.HPMN.

### Specification

If MDCR\_EL2.HPMN is set to 0, or to a value larger than PMCR\_ELO.N, then the value returned by a direct read of MDCR\_EL2.HPMN is **UNKNOWN**.

### Implementation

If MDCR\_EL2.HPMN is set to 0 or to a value larger than PMCR\_ELO.N, then an **UNKNOWN** number of counters are reserved for EL2 use. That is, the PE behaves as if MDCR\_EL2.HPMN is set to an **UNKNOWN** non-zero value less than or equal to PMCR\_ELO.N.

## C.6 The Activity Monitors Extension

This section describes the specification and implementation of the Activity Monitors Extension.

### Specification

If <n> is greater than the number of architected activity monitor event counters, reads and writes of AMEVCNTR0<n>\_ELO and AMEVTYPER0<n>\_ELO are **CONSTRAINED UNPREDICTABLE**.

### Implementation

The Activity Monitors Extension is not implemented in the Cortex®-R82AE processor.

## C.7 Syndrome register handling for **CONSTRAINED UNPREDICTABLE** instructions treated as **UNDEFINED**

This section describes the specification and implementation of the syndrome register handling.

### Specification

When a **CONSTRAINED UNPREDICTABLE** instruction is treated as **UNDEFINED**, ESR\_ELx is **UNKNOWN**.

### Implementation

**CONSTRAINED UNPREDICTABLE** instructions are not treated as **UNDEFINED** in the Cortex®-R82AE processor.

## C.8 Out of range virtual address

This section describes the specification and implementation of the out of range virtual address.

### Specification

If the PE executes a load or store instruction with tagged addressing disabled in the current translation regime, and where the computed virtual address, total access size, and alignment mean that it accesses the bytes at `0xFFFFFFFFFFFFFFFF` and `0x0000000000000000`, then the bytes that appear to be from `0x0000000000000000` onwards are accessed at an **UNKNOWN** address.

If the PE executes a load or store instruction with tagged addressing enabled in the current translation regime, and where the computed address, total access size, and alignment mean that it accesses the bytes at `0xFFFFFFFFFFFFFFFF` and `0x0000000000000000`, then the bytes that appear to be from `0x0000000000000000` onwards are accessed at an **UNKNOWN** address and the tags associated with address also become **UNKNOWN**.

### Implementation

Accesses to out of range virtual addresses cause an abort in the Cortex®-R82AE processor.

## C.9 Mapping of non-idempotent memory locations using the Normal memory type

This section describes the specification and implementation of mapping of non-idempotent memory locations using the Normal memory type.

### Specification

If non-idempotent memory locations are mapped using the Normal memory type, the state of the non-idempotent-memory location may become corrupted in following circumstances:

- Speculative read accesses may cause accesses to the non-idempotent memory locations that would not occur as part of a simple sequential execution.
- Writes to non-idempotent memory locations might be merged or split. In this case, the number and size of writes seen by the memory location might not be the number and size that occur as part of a simple sequential execution.

### Implementation

The Cortex®-R82AE processor implementation is the same as the specification.

## C.10 Instruction fetches from Device memory

This section describes the specification and implementation of instruction fetches from Device memory.

### Specification

Instruction fetches from Device memory are **CONSTRAINED UNPREDICTABLE**.

### Implementation

If a location in memory has the Device attribute and is not marked as execute-never, then the Cortex®-R82AE processor will report a permission fault.

## C.11 Programming the CSSELR\_EL1.Level for a cache level that is not implemented

This section describes the specification and implementation of programming the CSSELR\_EL1.Level for a cache level that is not implemented.

### Specification

If the CSSELR\_EL1.Level is programmed to a cache level that is not implemented, then a read of CSSELR\_EL1 returns an **UNKNOWN** value in CSSELR\_EL1.Level.

If CSSELR\_EL1.Level is programmed to a cache level that is not implemented, then on a read of CCSIDR\_EL1 an implementation must perform one of the following behaviors:

- The CCSIDR\_EL1 read is treated as a NOP.
- The CCSIDR\_EL1 read is **UNDEFINED**.
- The CCSIDR\_EL1 read returns an **UNKNOWN** value.

### Implementation

If the CSSELR\_EL1.Level is programmed to a cache level that is not implemented, then a read of CSSELR\_EL1 returns an **UNKNOWN** value in CSSELR\_EL1.Level.

If CSSELR\_EL1.Level is programmed to a cache level that is not implemented, then a read of CCSIDR\_EL1 returns an **UNKNOWN** value.

## C.12 Crossing a page boundary with different memory types or Shareability attributes

This section describes the specification and implementation of crossing a page boundary with different memory types or Shareability attributes.

### Specification

A memory access from a load or store instruction that crosses a page boundary to a memory location that has a different memory type or Shareability attribute results in **CONSTRAINED UNPREDICTABLE** behavior.

### Implementation

The Cortex®-R82AE processor has the following behavior for crossing a page (or translation) boundary with different memory types or Shareability attributes:

- Each memory access generated by the instruction uses the memory type and Shareability attribute associated with its own address.
- For alignment checking, the first address of the instruction is used. Therefore, if crossing from Normal to Device memory, an alignment fault would be taken on the second access if not aligned to element size. The Cortex®-R82AE processor treats any accesses that cross a 128-bit boundary as independent accesses, so all alignment, permission, and other fault checking is performed for each aligned 128-bit access. This means that if an access is permitted to the lower 128-bit aligned region but not to the higher 128-bit aligned region, then the first access will go ahead. This may mean that the lower addresses are updated if there is a store that gets a fault on the second access.

## C.13 CONSTRAINED UNPREDICTABLE behaviors with Load-Exclusive/Store-Exclusive pairs

This section describes the specification and implementation of Load-Exclusive/Store-Exclusive pairs.

Load-Exclusive and Store-Exclusive instruction usage restrictions in the Arm®v8 architecture defines a Load-Exclusive/Store-Exclusive pair, and identifies various **CONSTRAINED UNPREDICTABLE** behaviors associated with using Load-Exclusive/Store-Exclusive pairs. These cases and their implementation in the Cortex®-R82AE processor are:

- The target virtual address of a StoreExcl instruction is different from the virtual address of the preceding LoadExcl instruction in the same thread of execution.

### Implementation

This will cause the StoreExcl to fail, the status value returned by the StoreExcl is **UNKNOWN**, and the states of the local and global monitors for that PE are **UNKNOWN**. The data at the address accessed by the LoadExcl, and at the address accessed by the StoreExcl, is **UNKNOWN**.



- The transaction size of a StoreExcl instruction is different from the transaction size of the preceding LoadExcl instruction in the same thread of execution.

#### Implementation

The Cortex®-R82AE processor does not require the transaction size to be the same.

- The StoreExcl instruction accesses a different number of registers than the preceding LoadExcl instruction in the same thread of execution.

#### Implementation

The Cortex®-R82AE processor does not require that StoreExcl instruction access the same number of registers as the preceding LoadExcl instruction. Therefore a difference in the number of registers accessed does not affect whether a StoreExcl passes or fails.

- The memory attributes for a StoreExcl instruction are different from the memory attributes for the preceding LoadExcl instruction in the same thread of execution.

#### Implementation

If Cacheability or Shareability differs between the LoadExcl and the StoreExcl, the store exclusive will fail.

- The effect of a data or unified cache invalidate, clean, or clean and invalidate instruction on a local or global Exclusives monitor that is in the Exclusive Access state is **CONSTRAINED UNPREDICTABLE**.

#### Implementation

If the load exclusive is allocated into the cache and has shareable attributes, cache invalidation will cause the monitor to be opened.

## C.14 CONSTRAINED UNPREDICTABLE behavior for instructions

This section describes **CONSTRAINED UNPREDICTABLE** behavior for instructions.

### C.14.1 LDAXP, LDNP, LDNP (SIMD&FP)

This section describes the specification and implementation of LDAXP, LDNP, LDNP (SIMD&FP).

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If  $t == t2$ , then the instruction performs a load using the specified addressing mode, and the transfer register is set to an **UNKNOWN** value.

## C.14.2 LDP

This section describes the specification and implementation of LDP.

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If the instruction encoding specifies pre-indexed addressing or post-indexed addressing, and  $(t == n \parallel t2 == n) \&\& n \neq 31$ , then the instruction performs a load using the specified addressing mode, and the base register is set to an **UNKNOWN** value. In addition, if an exception occurs during such an instruction, the base register might be corrupted so that the instruction cannot be repeated.

If  $t == t2$ , then the instruction performs all of the loads using the specified addressing mode, and the transfer register is set to an **UNKNOWN** value.

## C.14.3 LDP (SIMD&FP)

This section describes the specification and implementation of LDP (SIMD&FP).

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If  $t == t2$ , then the instruction performs all of the loads using the specified addressing mode, and the transfer register is set to an **UNKNOWN** value.

## C.14.4 LDPSW

This section describes the specification and implementation of LDPSW.

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If the instruction encoding specifies pre-indexed addressing or post-indexed addressing, and  $(t == n \parallel t2 == n) \&\& n \neq 31$ , then the instruction performs a load using the specified addressing mode, and the base register is set to an **UNKNOWN** value. In addition, if an exception occurs during such an instruction, the base register might be corrupted so that the instruction cannot be repeated.

If  $t == t2$ , then the instruction performs all of the loads using the specified addressing mode, and the transfer register is set to an **UNKNOWN** value.

### C.14.5 LDR (immediate), LDRB (immediate), LDRH (immediate), LDRSB (immediate), LDRSH (immediate), LDRSW (immediate)

This section describes the specification and implementation of LDR (immediate), LDRB (immediate), LDRH (immediate), LDRSB (immediate), LDRSH (immediate), LDRSW (immediate).

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If the instruction encoding specifies pre-indexed addressing or post-indexed addressing, and  $n == t$  &&  $n != 31$ , then the instruction performs the load using the specified addressing mode, and the base register is set to an **UNKNOWN** value. In addition, if an exception occurs during such an instruction, the base register might be corrupted so that the instruction cannot be repeated.

### C.14.6 LDXP

This section describes the specification and implementation of LDXP.

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If  $t == t2$ , then the instruction performs a load using the specified addressing mode, and the transfer register is set to an **UNKNOWN** value.

### C.14.7 STP

This section describes the specification and implementation of STP.

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If the instruction encoding specifies pre-indexed addressing or post-indexed addressing, and  $(t == n \parallel t2 == n) \&\& n != 31$ , then the instruction performs a store using the specified addressing mode but the value stored is **UNKNOWN**.

## C.14.8 STLXP

This section describes the specification and implementation of STLXP.

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If  $s == t \parallel (s == t2)$ , then the instruction performs the store to the specified address, but the value stored is **UNKNOWN**.

If  $s == n \ \&\& \ n \neq 31$ , then the instruction performs the store to an **UNKNOWN** address.

## C.14.9 STLXR, STLXRB, STLXRH

This section describes the specification and implementation of STLXR, STLXRB, STLXRH.

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If  $s == t$ , then the instruction performs the store to the specified address, but the value stored is **UNKNOWN**.

If  $s == n \ \&\& \ n \neq 31$  then the instruction performs the store to an **UNKNOWN** address.

## C.14.10 STR (immediate), STRB (immediate), STRH (immediate)

This section describes the specification and implementation of STR (immediate), STRB (immediate), STRH (immediate).

### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

### Implementation

If the instruction encoding specifies pre-indexed addressing or post-indexed addressing, and  $n == t \ \&\& \ n \neq 31$ , then the instruction performs a store using the specified addressing mode but the value stored is **UNKNOWN**.

### C.14.11 STXP

This section describes the specification and implementation of STXP.

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If  $s == t \parallel (s == t2)$ , then the instruction performs the store to the specified address, but the value stored is **UNKNOWN**.

If  $s == n \ \&\& \ n \neq 31$  then the instruction performs the store to an **UNKNOWN** address.

### C.14.12 STXR, STXRB, STXRH

This section describes the specification and implementation of STXR, STXRB, STXRH.

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If  $s == t$ , then the instruction performs the store to the specified address, but the value stored is **UNKNOWN**.

If  $s == n \ \&\& \ n \neq 31$  then the instruction performs the store to an **UNKNOWN** address.

## C.15 Out of range values of the Set/Way/Index fields in cache maintenance instructions

This section describes the specification and implementation of Out of range values of the Set/Way/Index fields in cache maintenance instructions.

#### Specification

In the cache maintenance by set/way instructions `DC C1SW`, `DC C2SW`, and `DC ISW`, if any set/way/index argument is larger than the value supported by the implementation, then the behavior is **CONSTRAINED UNPREDICTABLE**.

#### Implementation

In this situation, the instruction performs cache maintenance on a single arbitrary cache line.

## C.16 Reserved values in System and memory-mapped registers and translation table entries

### Specification

Unless otherwise stated in the [Arm® Architecture Reference Manual for A-profile architecture](#), all unallocated or reserved values of fields with allocated values within AArch64 System registers, memory-mapped registers, and translation table entries behave in one of the following ways:

- The unallocated value maps onto any of the allocated values, but otherwise does not cause **CONSTRAINED UNPREDICTABLE** behavior.
- The unallocated value causes effects that could be achieved by a combination of more than one of the allocated values.
- The unallocated value causes the field to have no functional effect.

### Implementation

All unallocated or reserved values of fields with allocated values within AArch64 System registers, memory-mapped registers, and translation table entries have no functional effect.

## C.17 CONSTRAINED UNPREDICTABLE behavior in Debug state

This section describes the **CONSTRAINED UNPREDICTABLE** behaviors that are specifically associated with Debug state.

### C.17.1 Instructions that are CONSTRAINED UNPREDICTABLE in Debug state

This section lists instructions that are **CONSTRAINED UNPREDICTABLE** in Debug state and their implementation behavior.

- Exception-generating instructions  
These instructions are: SVC, HVC, BRK, HLT.

#### Implementation

They are **UNDEFINED**.

- Instructions that explicitly write to the PC  
These instructions are: B, B.cond, BL, BLR, BR, CBZ, CBNZ, RET, TBZ, TBNZ.

#### Implementation

They are **UNDEFINED**.

- Exception return ERET.

**Implementation**

They are **UNDEFINED**.

- Instructions that request entry to low-power state  
These instructions are: WFE, WFI.

**Implementation**

They are **UNDEFINED**.

- Instructions that read the PC  
These instructions are: LDR (literal), LDRSW (literal), ADR, ADRP, PRFM (literal).

**Implementation**

They are **UNDEFINED**.

- Instructions that explicitly modify PSTATE  
These instructions are:
  - ADDS, SUBS, ADCS, SBCS, ANDS, BICS, CCMN, CCMP
  - FCMP, FCMPE, FCCMP, FCCMPE
  - MSR DAIFSet (immediate), MSR DAIFClr (immediate), MSR SPSel (immediate)
  - MSR NZCV (register), MSR DAIF (register), MSR SPSel (register)
  - MSR PAN (immediate) and MSR PAN (register)
  - MSR UAO (immediate) and MSR UAO (register)
  - CFINV, RMIF, SETF8, SETF16
  - MSR DIT

**Implementation**

They are **UNDEFINED**.

- Instructions that read PSTATE.{N, Z, C, V} or other PSTATE fields  
These instructions are:
  - CSEL, CSINC, CSINV, CSNEG, CCMN, CCMP, FCSEL, FCCMP, FCCMPE
  - ADC, ADCS, SBC, SBCS
  - CFIINV
  - MRS NZCV, MRS DAIF, MRS SPSel, MRS CurrentEL
  - MSR PAN
  - MSR UAO
  - MSR DIT

**Implementation**

They are **UNDEFINED**.

- Hint instruction DGH.

**Implementation**

They execute as in Non-debug state.

- All other instructions that are not specified either as changed or unchanged in Debug state and are not listed above

**Implementation**

They are **UNDEFINED**.

## C.17.2 Exiting Debug state

This section describes the specification and implementation of exiting Debug state.

**Specification**

The PE exits Debug state when it receives a Restart request trigger event. If EDSCR.ITE == 0 the behavior of any instruction issued through the ITR in Normal access mode or an operation issued by a DTR access in memory access mode that has not completed execution is **CONSTRAINED UNPREDICTABLE**.

**Implementation**

In this case the Cortex®-R82AE processor completes execution in Debug state before the PE executes the restart sequence.

## C.17.3 Changing the value of EDECR.SS when not in Debug state

This section describes the specification and implementation of changing the value of EDECR.SS when not in Debug state.

**Specification**

If software changes the value of EDECR.SS when the PE is not in Debug state then behavior is **CONSTRAINED UNPREDICTABLE**.

**Implementation**

In this situation in the Cortex®-R82AE processor, the value of EDECR.SS becomes **UNKNOWN**.

## C.17.4 Syndrome information on Halting Step

This section describes the specification and implementation of Syndrome information on Halting Step.

EDSCR.STATUS is **CONSTRAINED UNPREDICTABLE** when:

- The instruction being stepped generated a Halting Step debug event before the instruction was executed.

**Implementation**

In this case EDSCR.STATUS is set to:

- Halting Step, no syndrome, if the stepped instruction was not a Load-Exclusive instruction



- Halting Step, no syndrome, if the stepped instruction was a Load-Exclusive instruction
- The instruction that was stepped was an Exception Return instruction or an ISB.

#### Implementation

In this case EDSCR.STATUS is set to Halting Step, no syndrome.

### C.17.5 Illegal Execution state exception

This section describes the specification and implementation of Illegal Execution state exception.

#### Specification

If PSTATE.IL is set to 1 when EDSCR.MA == 1, then on an external write access to DBGDTRRX\_ELO or an external read from DBGDTRTX\_ELO, it is **CONSTRAINED UNPREDICTABLE**.

#### Implementation

The Cortex®-R82AE processor ignores PSTATE.IL.

### C.17.6 Alignment constraints

This section describes the specification and implementation of alignment constraints.

#### Specification

See *CONSTRAINED UNPREDICTABLE behavior for A64 instructions* chapter of the [Arm® Architecture Reference Manual for A-profile architecture](#).

#### Implementation

If the address in R0 is not aligned to a multiple of four, the Cortex®-R82AE processor makes an unaligned memory access to R0. If alignment checking is enabled for the memory access, this generates an Alignment fault.

### C.17.7 Cumulative error flag

This section describes the specification and implementation of cumulative error flag.

#### Specification

The cumulative error flag remains set until cleared to 0 by writing 1 to EDRCCR.CSE. However, the effect of writing 1 to EDRCCR.CSE to clear EDSCR.ERR is **CONSTRAINED UNPREDICTABLE** when both of the following apply:

- The PE is in Debug state
- The value of EDSCR.ITE is 0

#### Implementation

When these conditions apply and a value of 1 is written to EDRCCR.CSE, the Cortex®-R82AE processor clears the cumulative error flag EDSCR.ERR.

### C.17.8 Restart request trigger event

This section describes the specification and implementation of Restart request trigger event.

#### Specification

If a Restart request trigger event is received at or about the same time as the PE enters Debug state, it is **CONSTRAINED UNPREDICTABLE** whether:

- The request is ignored by the PE. In this case the PE enters Debug state and remains in Debug state.
- The PE enters Debug state and then immediately restarts.

#### Implementation

The Cortex®-R82AE processor enters Debug state and then immediately restarts.

### C.17.9 External debug interface accesses to registers in reset

This section describes the specification and implementation of external debug interface accesses to registers in reset.

#### Specification

If a reset signal is asserted and the external debug interface writes a register, or indirectly writes a register or register field as a side-effect of an access:

- Then, if the register or register field is reset by that reset signal, it is **CONSTRAINED UNPREDICTABLE** whether the register or register field takes the reset value or the value written. The reset value might be **UNKNOWN**.
- Otherwise, the register or register field takes the value that is written.

#### Implementation

In this case in the Cortex®-R82AE processor, the register or register field takes the reset value.

### C.17.10 Reserved and unallocated registers

This section describes the specification and implementation of reserved and unallocated registers.

#### Specification

See [Arm® Architecture Reference Manual for A-profile architecture](#) for information on reserved and unallocated registers.

#### Implementation

For reserved Debug registers and Performance Monitors registers, if the core power domain is off state, the response is an Error. If the core is in retention, these accesses initiate a wakeup and the response is not an Error.

### C.17.11 External accesses to DBGBVR<n>\_EL1 and DBGBCR<n>\_EL1

This section describes the specification and implementation of external accessing to DBGBVR<n>\_EL1 and DBGBCR<n>\_EL1.

#### Specification

See [Arm® Architecture Reference Manual for A-profile architecture](#) for information on external accesses to DBGBVR<n>\_EL1 and DBGBCR<n>\_EL1.

#### Implementation

If breakpoint n is not implemented then accesses to these registers return an Error if either core is off, or `os_Lock` is set, or `AllowExternalDebugAccess()` is false.

### C.17.12 External accesses to DBGWVR<n>\_EL1 and DBGWCR<n>\_EL1

This section describes the specification and implementation of external accessing to DBGWVR<n>\_EL1 and DBGWCR<n>\_EL1.

#### Specification

See [Arm® Architecture Reference Manual for A-profile architecture](#) for information on external accesses to DBGWVR<n>\_EL1 and DBGWCR<n>\_EL1.

#### Implementation

If watchpoint n is not implemented then accesses to these registers return an Error if either core is off, or `os_Lock` is set, or `AllowExternalDebugAccess()` is false.

### C.17.13 Accessing the EDESR

This section describes the specification and implementation of accessing the EDESR.

#### Specification

If a request to clear a pending Halting debug event is received at or about the time when halting becomes allowed, it is **CONSTRAINED UNPREDICTABLE** whether the event is taken.

#### Implementation

In this case, the event is not taken.

### C.17.14 Accessing the CTIAPPPULSE

This section describes the specification and implementation of accessing the CTIAPPPULSE.

#### Specification

It is **CONSTRAINED UNPREDICTABLE** whether a write to CTIAPPPULSE generates an event on a channel if `CTICONTROL.GLBEN` is 0.

## Implementation

In this case, the Cortex®-R82AE processor will not generate an output channel event

## C.18 RAS registers

In ERR<n>MISC0, Error Record Miscellaneous Register 0, the Corrected Error Counter CEC[38:32] counts only Corrected errors.

Deferred and Uncorrected errors are not counted.

See [B.1.2.1.4 ERR<n>MISC0, Error Record <n> Miscellaneous Register 0, n = 0 - 9](#) on page 1520 for more information.

# Appendix D Generic handler example

This appendix contains example interrupt handling sequences.

## D.1 Generic handler example, part 1

An example generic handler preamble code snippet is provided here, under the following assumptions:

- No branch required from the exception vector address, because the generic interrupt handler preamble can wholly fit (it is less than 32 instructions, or 0x80 bytes); if a bigger preamble is needed, a branch instruction can be added.
- Re-entrant interrupts are desirable; if not, the SPSR/ELR saving and the DAIFCLR access can be omitted.
- Non-generic interrupt handler does not use FP/NEON registers; if it needs to, the caller-saved FP/NEON registers must be saved as well.
- The handler-specific stack is used; if the thread-specific stack is needed instead, an `MSR SPSEL` instruction must be added.

This example shows the preamble of an EL1 interrupt handler for IRQ. A similar code snippet could be applicable for EL2 and/or FIQ or asynchronous aborts. The code has been optimized to take advantage of the superscalar capabilities in the Cortex®-R82AE processor, for example, instructions have been organized to allow for maximal multi-issuing.

```
// Save the first batch of the caller-saved registers to the stack.
STP X1, X2, [SP, #-16]!
STP X0, X3, [SP, #-16]!

// Read the ID of the highest-priority interrupt in X0,
// and acknowledge the interrupt.
// Read the exception context in X1 and X2.
// Meanwhile, continue saving caller-saved registers.
MRS X0, ICC_IAR0_EL1
STP X4, X5, [SP, #-16]!
MRS X1, SPSR_EL1
STP X6, X7, [SP, #-16]!
MRS X2, ELR_EL1
STP X8, X9, [SP, #-16]!

// Re-enable IRQ interrupts. Higher-priority interrupts can now be taken.
MSR DAIFCLR, #2

// Save the rest of the caller-saved registers.
// We have already done X0-X9, but we are saving again X0-X2 that contain
// the interrupt ID and the exception context. We will need them again after
// the non-generic handler returns, to end the interrupt and
// to perform the exception return.
//
// Meanwhile, find the correct non-generic interrupt handler function
// for this IRQ by looking up the interrupt ID in a table of handlers.
// In C notation, the computed function address is X3 = irq_table_base[X0 * 8].
STP X10, X11, [SP, #-16]!
STP X12, X13, [SP, #-16]!
ADR X3, irq_table_base
```

```

STP X14, X15, [SP, #-16]!
ADD X3, X3, X0, LSL #3
STP X16, X17, [SP, #-16]!
STP X29, X30, [SP, #-16]!
LDR X3, [X3]
STP X1, X2, [SP, #-16]!
STP X0, X18, [SP, #-16]!

// Branch to non-generic handler.
// Interrupt ID is passed as the first argument in X0.
// SPSR and ELR are passed as arguments in X1 and X2 as well.
BLR X3

// Branch to epilogue code, if it cannot fit in the exception vector.
B generic_handler_epilogue

```

## D.2 Generic handler example, part 2

After the non-generic handler function returns, an example generic handler epilogue is provided in the following code snippet. The example continues the EL1 IRQ handler example with similar assumptions. This example epilogue cannot fit together with the example preamble in the exception vector address, as their combined size is slightly more than 32 instructions. For this reason, a branch is assumed to be required after the non-generic handler return to point to the epilogue code that is in another memory section.

```

// Restore the interrupt ID (X0) and the exception context (X1, X2).
// Also restore the caller-saved X18, to take advantage of load-pair instructions.
generic_handler_epilogue:
LDP X0, X18, [SP], #16
LDP X1, X2, [SP], #16

// Tell the GIC that this interrupt ID has been handled, and it can be deactivated.
// Note that if the source of the interrupt has to be cleared,
// this has already been taken care of in the non-generic interrupt handler.
MSR ICC_EOIR0_EL1, X0

// Continue restoring caller-saved registers.
LDP X29, X30, [SP], #16
LDP X16, X17, [SP], #16
LDP X14, X15, [SP], #16
LDP X12, X13, [SP], #16
LDP X10, X11, [SP], #16
LDP X8, X9, [SP], #16
LDP X6, X7, [SP], #16
LDP X4, X5, [SP], #16
LDP X0, X3, [SP], #16

// Restore the SPSR and ELR so that we can return from the exception.
// Disable interrupts before doing this, to avoid another interrupt corrupting them.
MSR DAIFSet, #2
MSR SPSR_EL1, X1
MSR ELR_EL1, X2

// Restore remaining caller-saved registers.
LDP X1, X2, [SP], #16

// Return from the exception.
ERET

```

# Proprietary Notice

This document is protected by copyright and other related rights and the use or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm Limited ("Arm"). No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether the subject matter of this document infringes any third party patents.

The content of this document is informational only. Any solutions presented herein are subject to changing conditions, information, scope, and data. This document was produced using reasonable efforts based on information available as of the date of issue of this document. The scope of information in this document may exceed that which Arm is required to provide, and such additional information is merely intended to further assist the recipient and does not represent Arm's view of the scope of its obligations. You acknowledge and agree that you possess the necessary expertise in system security and functional safety and that you shall be solely responsible for compliance with all legal, regulatory, safety and security related requirements concerning your products, notwithstanding any information or support that may be provided by Arm herein. In addition, you are responsible for any applications which are used in conjunction with any Arm technology described in this document, and to minimize risks, adequate design and operating safeguards should be provided for by you.

This document may include technical inaccuracies or typographical errors. THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, any patents, copyrights, trade secrets, trademarks, or other rights.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Reference by Arm to any third party's products or services within this document is not an express or implied approval or endorsement of the use thereof.

This document consists solely of commercial items. You shall be responsible for ensuring that any permitted use, duplication, or disclosure of this document complies fully with any relevant

export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word “partner” in reference to Arm’s customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of this document shall prevail.

The validity, construction and performance of this notice shall be governed by English Law.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its affiliates) in the US and/or elsewhere. Please follow Arm’s trademark usage guidelines at <https://www.arm.com/company/policies/trademarks>. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

PRE-1121-V1.0



# Product and document information

Read the information in these sections to understand the release status of the product and documentation, and the conventions used in the Arm documents.

## Product status

All products and Services provided by Arm require deliverables to be prepared and made available at different levels of completeness. The information in this document indicates the appropriate level of completeness for the associated deliverables.

### Product completeness status

The information in this document is Final, that is for a developed product.

### Product revision status

This product is rOp1, which indicates the revision status of the product described in this manual, where:

- r (value)** Identifies the major revision of the product, for example, r1.
- p (value)** Identifies the minor revision or modification status of the product, for example, p2.

## Revision history

These sections can help you understand how the document has changed over time.

### Document release information

The Document history table gives the issue number and the released date for each released issue of this document.

#### Document history

Issue	Date	Confidentiality	Change
0001-04	28 March 2025	Non-Confidential	Second release for rOp1
0001-03	25 October 2024	Non-Confidential	First release for rOp1
0000-02	19 March 2024	Non-Confidential	First early access release for rOp0
0000-01	30 June 2023	Confidential	First beta release for rOp0

The Change history tables describe the technical changes between released issues of this document in reverse order. Issue numbers match the revision history in [Document release information](#) on page 2309.

**Table 2: Issue 0000-02**

Change	Location
First early access release for r0p0	-

**Table 3: Differences between Issue 0000-02 and Issue 0001-03**

Change	Location
First release for r0p1	-
Front matter and back matter order change	A change was made to the ordering of the front matter and back matter.
Architectural registers were updated with relevant changes for this release.	<a href="#">A. AArch64 registers</a> on page 307
External registers were updated with relevant changes for this release.	<a href="#">B. External registers</a> on page 1496
Memory Systems Chapter was updated with release correct specifications in every table throughout.	<a href="#">8. Memory system</a> on page 120
PMU events were updated with release correct specifications.	<a href="#">14. PMU</a> on page 276
Processor features chapter was revised to ensure clarity of text.	<a href="#">2. Technical overview</a> on page 40

**Table 4: Differences between Issue 0001-03 and Issue 0001-04**

Change	Location
Second release for r0p1	-
External registers were updated with relevant changes for this release.	<a href="#">B. External registers</a> on page 1496
Minor editorial changes.	Entire document

## Conventions

The following subsections describe conventions used in Arm documents.

### Glossary

The Arm Glossary is a list of terms used in Arm documentation, together with definitions for those terms. The Arm Glossary does not contain terms that are industry standard unless the Arm meaning differs from the generally accepted meaning.

See the Arm Glossary for more information: [developer.arm.com/glossary](https://developer.arm.com/glossary).

### Typographic conventions

Arm documentation uses typographical conventions to convey specific meaning.

Convention	Use
<i>italic</i>	Citations.
<b>bold</b>	Terms in descriptive lists, where appropriate.

Convention	Use
monospace	Text that you can enter at the keyboard, such as commands, file and program names, and source code.
monospace <u>underline</u>	A permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.
<and>	Encloses replaceable terms for assembler syntax where they appear in code or code fragments.  For example: <div>MRC p15, 0, &lt;Rd&gt;, &lt;CRn&gt;, &lt;CRm&gt;, &lt;Opcode_2&gt;</div>
SMALL CAPITALS	Terms that have specific technical meanings as defined in the <i>Arm® Glossary</i> . For example, <b>IMPLEMENTATION DEFINED</b> , <b>IMPLEMENTATION SPECIFIC</b> , <b>UNKNOWN</b> , and <b>UNPREDICTABLE</b> .



We recommend the following. If you do not follow these recommendations your system might not work.



Your system requires the following. If you do not follow these requirements your system will not work.



You are at risk of causing permanent damage to your system or your equipment, or of harming yourself.



This information is important and needs your attention.



This information might help you perform a task in an easier, better, or faster way.



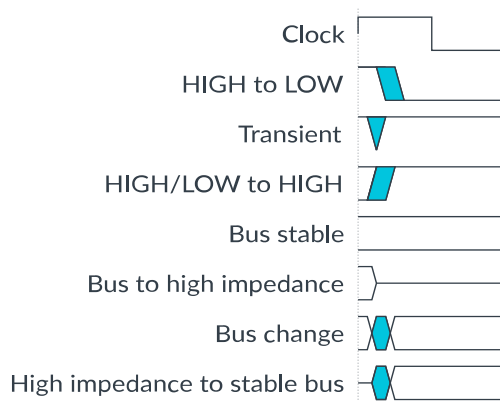
This information reminds you of something important relating to the current content.

## Timing diagrams

The following figure explains the components used in timing diagrams. Variations, when they occur, have clear labels. You must not assume any timing information that is not explicit in the diagrams.

Shaded bus and signal areas are undefined, so the bus or signal can assume any value within the shaded area at that time. The actual level is unimportant and does not affect normal operation.

**Figure 1: Key to timing diagram conventions**



## Signals

The signal conventions are:

### Signal level

The level of an asserted signal depends on whether the signal is active-HIGH or active-LOW. Asserted means:

- HIGH for active-HIGH signals.
- LOW for active-LOW signals.

### Lowercase n

At the start or end of a signal name, n denotes an active-LOW signal.

# Useful resources

This document contains information that is specific to this product. See the following resources for other useful information.

Access to Arm documents depends on their confidentiality:

- Non-Confidential documents are available at [developer.arm.com/documentation](https://developer.arm.com/documentation). Each document link in the following tables goes to the online version of the document.
- Confidential documents are available to licensees only through the product package.

Arm product resources	Document ID	Confidentiality
<a href="#">Arm® Cortex®-R82AE Configuration and Integration Manual</a>	101551	Confidential

Arm architecture and specifications	Document ID	Confidentiality
<a href="#">Arm® Architecture Reference Manual Supplement Armv8, for R-profile AArch64 architecture</a>	DDI 0600	Non-Confidential
<a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>	DDI 0487	Non-Confidential
<a href="#">AMBA® AXI Protocol Specification</a>	IHI 0022	Non-Confidential
<a href="#">AMBA® CHI Architecture Specification</a>	IHI 0050	Non-Confidential
<a href="#">AMBA® AXI-Stream Protocol Specification</a>	IHI 0051	Non-Confidential
<a href="#">AMBA® APB Protocol Specification</a>	IHI 0024	Non-Confidential
<a href="#">Arm® AMBA® 4 ATB Protocol Specification ATBv1.0 and ATBv1.1</a>	IHI 0032	Non-Confidential
<a href="#">AMBA® Low Power Interface Specification</a>	IHI 0068	Non-Confidential
<a href="#">Arm® Power Policy Unit Architecture Specification</a>	DEN 0051	Non-Confidential
<a href="#">Arm® CoreSight™ Architecture Specification v3.0</a>	IHI 0029	Non-Confidential
<a href="#">Arm® Embedded Trace Macrocell Architecture Specification ETMv4.0 to ETM4.6</a>	IHI 0064	Non-Confidential
<a href="#">Arm® Generic Interrupt Controller Architecture Specification, GIC architecture version 3 and version 4</a>	IHI 0069	Non-Confidential
<a href="#">Arm® Architecture Reference Manual Supplement Reliability, Availability, and Serviceability (RAS), for A-profile architecture</a>	DDI 0587	Non-Confidential
<a href="#">Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual</a>	101088	Non-Confidential

Non-Arm resources	Document ID	Organization
-	-	-