

ARM[®] Cortex-A34 Processor

Revision: r0p1

Technical Reference Manual



ARM® Cortex-A34 Processor

Technical Reference Manual

Copyright © 2016, 2017 ARM Limited or its affiliates. All rights reserved.

Release Information

Document History

Issue	Date	Confidentiality	Change
0000-00	18 March 2016	Confidential	First release for r0p0
0001-00	04 March 2017	Non-Confidential	First release for r0p1

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice 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. **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 implementations infringe any third party patents.

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, third party patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

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.

This document consists solely of commercial items. You shall be responsible for ensuring that any 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.

If any of the provisions contained in these terms conflict with any of the provisions of any signed written agreement covering this document with ARM, then the signed written agreement prevails over and supersedes the conflicting provisions of these terms. 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 the Agreement shall prevail.

Words and logos marked with ® or ™ are registered trademarks or trademarks of ARM Limited or its affiliates in the EU and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow ARM’s trademark usage guidelines at <http://www.arm.com/about/trademark-usage-guidelines.php>

Copyright © 2016, 2017, ARM Limited or its affiliates. All rights reserved.

ARM Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

LES-PRE-20349

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by ARM and the party that ARM delivered this document to.

Unrestricted Access is an ARM internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Web Address

<http://www.arm.com>

Contents

ARM® Cortex-A34 Processor Technical Reference Manual

Preface

<i>About this book</i>	16
<i>Feedback</i>	20

Part A **Functional Description**

Chapter A1

Introduction

A1.1	<i>About the Cortex-A34 processor</i>	A1-24
A1.2	<i>Features</i>	A1-25
A1.3	<i>Implementation options</i>	A1-26
A1.4	<i>Supported standards and specifications</i>	A1-28
A1.5	<i>Test features</i>	A1-29
A1.6	<i>Design tasks</i>	A1-30
A1.7	<i>Product revisions</i>	A1-31

Chapter A2

Technical Overview

A2.1	<i>Components</i>	A2-34
A2.2	<i>Interfaces</i>	A2-38
A2.3	<i>About system control</i>	A2-40
A2.4	<i>About the Generic Timer</i>	A2-41
A2.5	<i>About the memory model</i>	A2-42

Chapter A3	Clocks, Resets, and Input Synchronization	
A3.1	Clocks	A3-44
A3.2	Input synchronization	A3-45
A3.3	Resets	A3-46
Chapter A4	Power Management	
A4.1	Power domains	A4-50
A4.2	Power modes	A4-53
A4.3	Core Wait for Interrupt	A4-54
A4.4	Core Wait for Event	A4-55
A4.5	L2 Wait for Interrupt	A4-56
A4.6	Powering down an individual core	A4-57
A4.7	Powering up an individual core	A4-58
A4.8	Powering down the processor without system driven L2 flush	A4-59
A4.9	Powering up the processor without system driven L2 flush	A4-60
A4.10	Powering down the processor with system driven L2 flush	A4-61
A4.11	Powering up the processor with system driven L2 flush	A4-62
A4.12	Entering Dormant mode	A4-63
A4.13	Exiting Dormant mode	A4-64
A4.14	Event communication using WFE or SEV	A4-65
A4.15	Communication to the Power Management Controller	A4-66
A4.16	STANDBYWFI[3:0] and STANDBYWFIL2 signals	A4-67
A4.17	Q-channel	A4-68
Chapter A5	Cache Behavior and Cache Protection	
A5.1	Cached memory types	A5-70
A5.2	Coherency between data caches with the MOESI protocol	A5-71
A5.3	Cache misses, unexpected cache hits, and speculative fetches	A5-72
A5.4	Disabling a cache	A5-73
A5.5	Invalidating or cleaning a cache	A5-74
A5.6	About read allocate mode	A5-75
A5.7	About cache protection	A5-76
A5.8	Error reporting	A5-78
A5.9	Error injection	A5-79
Chapter A6	L1 Memory System	
A6.1	About the L1 memory system	A6-82
A6.2	TLB Organization	A6-83
A6.3	Program flow prediction	A6-84
A6.4	About the internal exclusive monitor	A6-85
A6.5	About data prefetching	A6-86
Chapter A7	L2 Memory System	
A7.1	About the L2 memory system	A7-88
A7.2	Snoop and maintenance requests	A7-90
A7.3	Support for memory types	A7-91
A7.4	Memory type information exported from the processor	A7-92
A7.5	Handling of external aborts	A7-93

Chapter A8

AXI Master Interface

A8.1	About the AXI master interface	A8-96
A8.2	AXI privilege information	A8-97
A8.3	AXI transactions	A8-98
A8.4	Attributes of the AXI master interface	A8-100

Chapter A9

ACE Master Interface

A9.1	About the ACE master interface	A9-104
A9.2	ACE configurations	A9-105
A9.3	ACE privilege information	A9-106
A9.4	ACE transactions	A9-107
A9.5	Attributes of the ACE master interface	A9-110
A9.6	Snoop channel properties	A9-112
A9.7	AXI compatibility mode	A9-113

Chapter A10

CHI Master Interface

A10.1	About the CHI master interface	A10-116
A10.2	CHI configurations	A10-117
A10.3	Attributes of the CHI master interface	A10-118
A10.4	CHI channel properties	A10-120
A10.5	CHI transactions	A10-121

Chapter A11

ACP Slave Interface

A11.1	About the ACP	A11-126
A11.2	Transfer size support	A11-127
A11.3	ACP performance	A11-128
A11.4	ACP user signals	A11-129

Chapter A12

GIC CPU Interface

A12.1	Bypassing the GIC CPU Interface	A12-132
A12.2	Memory map for the GIC CPU interface	A12-133

Part B

Register Descriptions

Chapter B1

AArch64 system registers

B1.1	AArch64 register summary	B1-140
B1.2	AArch64 Identification registers	B1-141
B1.3	AArch64 Exception handling registers	B1-142
B1.4	AArch64 Virtual memory control registers	B1-143
B1.5	AArch64 Other System control registers	B1-145
B1.6	AArch64 Cache maintenance operations	B1-146
B1.7	AArch64 TLB maintenance operations	B1-147
B1.8	AArch64 Address translation operations	B1-148
B1.9	AArch64 Miscellaneous operations	B1-149
B1.10	AArch64 Performance monitor registers	B1-150
B1.11	AArch64 Reset registers	B1-152
B1.12	AArch64 Secure registers	B1-153
B1.13	AArch64 Virtualization registers	B1-154
B1.14	AArch64 EL2 TLB maintenance operations	B1-155
B1.15	AArch64 GIC system registers	B1-156

B1.16	AArch64 Generic Timer registers	B1-158
B1.17	AArch64 Thread registers	B1-159
B1.18	AArch64 Implementation defined registers	B1-160
B1.19	Auxiliary Control Register, EL1	B1-162
B1.20	Auxiliary Control Register, EL2	B1-163
B1.21	Auxiliary Control Register, EL3	B1-165
B1.22	Auxiliary Fault Status Register 0, EL1, EL2, and EL3	B1-167
B1.23	Auxiliary Fault Status Register 1, EL1, EL2, and EL3	B1-168
B1.24	Auxiliary ID Register, EL1	B1-169
B1.25	Auxiliary Memory Attribute Indirection Register, EL1	B1-170
B1.26	Auxiliary Memory Attribute Indirection Register, EL2	B1-171
B1.27	Auxiliary Memory Attribute Indirection Register, EL3	B1-172
B1.28	Configuration Base Address Register, EL1	B1-173
B1.29	Cache Size ID Register, EL1	B1-174
B1.30	Cache Level ID Register, EL1	B1-176
B1.31	Architectural Feature Access Control Register, EL1	B1-178
B1.32	Architectural Feature Trap Register, EL2	B1-180
B1.33	Architectural Feature Trap Register, EL3	B1-182
B1.34	CPU Auxiliary Control Register, EL1	B1-184
B1.35	CPU Extended Control Register, EL1	B1-187
B1.36	CPU Memory Error Syndrome Register, EL1	B1-189
B1.37	Cache Type Register, EL0	B1-192
B1.38	Data Cache Zero ID Register, EL0	B1-194
B1.39	Exception Syndrome Register, EL1	B1-195
B1.40	Exception Syndrome Register, EL2	B1-197
B1.41	Exception Syndrome Register, EL3	B1-199
B1.42	Fault Address Register, EL1	B1-201
B1.43	Fault Address Register, EL2	B1-202
B1.44	Fault Address Register, EL3	B1-203
B1.45	Hyp Auxiliary Configuration Register, EL2	B1-204
B1.46	Hypervisor Configuration Register, EL2	B1-205
B1.47	Hypervisor IPA Fault Address Register, EL2	B1-211
B1.48	Hyp System Trap Register, EL2	B1-212
B1.49	AArch64 Debug Feature Register 0, EL1	B1-213
B1.50	AArch64 Instruction Set Attribute Register 0, EL1	B1-215
B1.51	AArch64 Processor Feature Register 0, EL1	B1-217
B1.52	AArch64 Memory Model Feature Register 0, EL1	B1-219
B1.53	Interrupt Status Register, EL1	B1-221
B1.54	L2 Auxiliary Control Register, EL1	B1-222
B1.55	L2 Control Register, EL1	B1-224
B1.56	L2 Extended Control Register, EL1	B1-226
B1.57	L2 Memory Error Syndrome Register, EL1	B1-228
B1.58	Memory Attribute Indirection Register, EL1	B1-231
B1.59	Memory Attribute Indirection Register, EL2	B1-233
B1.60	Memory Attribute Indirection Register, EL3	B1-234
B1.61	Monitor Debug Configuration Register, EL2	B1-235
B1.62	Monitor Debug Configuration Register, EL3	B1-238
B1.63	Monitor Debug System Control Register, EL1	B1-240
B1.64	Main ID Register, EL1	B1-243
B1.65	Multiprocessor Affinity Register, EL1	B1-245

B1.66	Physical Address Register, EL1	B1-247
B1.67	Revision ID Register, EL1	B1-250
B1.68	Reset Management Register, EL3	B1-251
B1.69	Reset Vector Base Address Register, EL3	B1-252
B1.70	Secure Configuration Register, EL3	B1-253
B1.71	System Control Register, EL1	B1-256
B1.72	System Control Register, EL2	B1-259
B1.73	System Control Register, EL3	B1-261
B1.74	Translation Control Register, EL1	B1-263
B1.75	Translation Control Register, EL2	B1-267
B1.76	Translation Control Register, EL3	B1-269
B1.77	Translation Table Base Register 0, EL1	B1-271
B1.78	Translation Table Base Register 0, EL3	B1-272
B1.79	Translation Table Base Register 1, EL1	B1-273
B1.80	Vector Base Address Register, EL1	B1-274
B1.81	Vector Base Address Register, EL2	B1-275
B1.82	Vector Base Address Register, EL3	B1-276
B1.83	Virtualization Multiprocessor ID Register, EL2	B1-277
B1.84	Virtualization Processor ID Register, EL2	B1-278
B1.85	Virtualization Translation Control Register, EL2	B1-279

Chapter B2

GIC registers

B2.1	CPU interface register summary	B2-282
B2.2	Active Priority Register	B2-283
B2.3	CPU Interface Identification Register	B2-284
B2.4	Virtual interface control register summary	B2-285
B2.5	VGIC Type Register	B2-286
B2.6	Virtual CPU interface register summary	B2-287
B2.7	VM Active Priority Register	B2-288
B2.8	VM CPU Interface Identification Register	B2-289

Chapter B3

Generic Timer registers

B3.1	AArch64 Generic Timer register summary	B3-292
------	----------------------------------------------	--------

Part C

Debug

Chapter C1

Debug

C1.1	About debug methods	C1-296
C1.2	Debug access	C1-297
C1.3	Effects of resets on debug registers	C1-298
C1.4	External access permissions to debug registers	C1-299
C1.5	Debug events	C1-300
C1.6	Debug memory map	C1-301
C1.7	Debug signals	C1-303
C1.8	Changing the authentication signals for debug	C1-304

Chapter C2

PMU

C2.1	About the PMU	C2-306
C2.2	External register access permissions to the PMU registers	C2-307
C2.3	Performance monitoring events	C2-308

	C2.4	PMU interrupts	C2-312
	C2.5	Exporting PMU events	C2-313
Chapter C3		ETM	
	C3.1	About the ETM	C3-316
	C3.2	Configuration options for the ETM unit and trace resources	C3-318
	C3.3	Resetting the ETM	C3-320
	C3.4	Programming and reading ETM trace unit registers	C3-321
Chapter C4		CTI	
	C4.1	About the cross-trigger	C4-324
	C4.2	Cross-trigger inputs and outputs	C4-325
Chapter C5		Direct access to internal memory	
	C5.1	About direct access to internal memory	C5-328
	C5.2	Encoding for tag and data in the L1 instruction cache	C5-329
	C5.3	Encoding for tag and data in the L1 data cache	C5-330
	C5.4	Encoding for the main TLB RAM	C5-332
	C5.5	Encoding for walk cache	C5-337
	C5.6	Encoding for IPA cache	C5-338
Chapter C6		Debug AArch64 registers	
	C6.1	AArch64 debug register summary	C6-340
	C6.2	Debug Breakpoint Control Registers, EL1	C6-342
	C6.3	Debug Watchpoint Control Registers, EL1	C6-345
	C6.4	Debug Claim Tag Set register, EL1	C6-347
Chapter C7		Debug memory mapped registers	
	C7.1	Memory-mapped debug register summary	C7-350
	C7.2	External Debug Reserve Control Register	C7-354
	C7.3	External Debug Integration Mode Control Register	C7-355
	C7.4	External Debug Device ID Register 0	C7-356
	C7.5	External Debug Device ID Register 1	C7-357
	C7.6	External Debug Processor Feature Register	C7-358
	C7.7	External Debug Feature Register	C7-360
	C7.8	External Debug Peripheral Identification Registers	C7-362
	C7.9	External Debug Peripheral Identification Register 0	C7-363
	C7.10	External Debug Peripheral Identification Register 1	C7-364
	C7.11	External Debug Peripheral Identification Register 2	C7-365
	C7.12	External Debug Peripheral Identification Register 3	C7-366
	C7.13	External Debug Peripheral Identification Register 4	C7-367
	C7.14	External Debug Peripheral Identification Register 5-7	C7-368
	C7.15	External Debug Component Identification Registers	C7-369
	C7.16	External Debug Component Identification Register 0	C7-370
	C7.17	External Debug Component Identification Register 1	C7-371
	C7.18	External Debug Component Identification Register 2	C7-372
	C7.19	External Debug Component Identification Register 3	C7-373
Chapter C8		ROM table	
	C8.1	About the ROM table	C8-376
	C8.2	ROM table register interface	C8-377

C8.3	ROM table register summary	C8-378
C8.4	ROM entry registers	C8-379
C8.5	ROM Table Peripheral Identification Registers	C8-382
C8.6	ROM Table Peripheral Identification Register 0	C8-383
C8.7	ROM Table Peripheral Identification Register 1	C8-384
C8.8	ROM Table Peripheral Identification Register 2	C8-385
C8.9	ROM Table Peripheral Identification Register 3	C8-386
C8.10	ROM Table Peripheral Identification Register 4	C8-387
C8.11	ROM Table Peripheral Identification Register 5-7	C8-388
C8.12	ROM Table Component Identification Registers	C8-389
C8.13	ROM Table Component Identification Register 0	C8-390
C8.14	ROM Table Component Identification Register 1	C8-391
C8.15	ROM Table Component Identification Register 2	C8-392
C8.16	ROM Table Component Identification Register 3	C8-393

Chapter C9

PMU registers

C9.1	AArch64 PMU register summary	C9-396
C9.2	Performance Monitors Control Register, EL0	C9-397
C9.3	Performance Monitors Common Event Identification Register 0, EL0	C9-399
C9.4	Performance Monitors Common Event Identification Register 1, EL0	C9-403
C9.5	Memory-mapped PMU register summary	C9-405
C9.6	Performance Monitors Configuration Register	C9-408
C9.7	Performance Monitors Peripheral Identification Registers	C9-409
C9.8	Performance Monitors Peripheral Identification Register 0	C9-410
C9.9	Performance Monitors Peripheral Identification Register 1	C9-411
C9.10	Performance Monitors Peripheral Identification Register 2	C9-412
C9.11	Performance Monitors Peripheral Identification Register 3	C9-413
C9.12	Performance Monitors Peripheral Identification Register 4	C9-414
C9.13	Performance Monitors Peripheral Identification Register 5-7	C9-415
C9.14	Performance Monitors Component Identification Registers	C9-416
C9.15	Performance Monitors Component Identification Register 0	C9-417
C9.16	Performance Monitors Component Identification Register 1	C9-418
C9.17	Performance Monitors Component Identification Register 2	C9-419
C9.18	Performance Monitors Component Identification Register 3	C9-420

Chapter C10

ETM registers

C10.1	ETM register summary	C10-423
C10.2	Programming Control Register	C10-426
C10.3	Status Register	C10-427
C10.4	Trace Configuration Register	C10-428
C10.5	Branch Broadcast Control Register	C10-430
C10.6	Auxiliary Control Register	C10-431
C10.7	Event Control 0 Register	C10-433
C10.8	Event Control 1 Register	C10-435
C10.9	Stall Control Register	C10-436
C10.10	Global Timestamp Control Register	C10-437
C10.11	Synchronization Period Register	C10-438
C10.12	Cycle Count Control Register	C10-439
C10.13	Trace ID Register	C10-440
C10.14	ViewInst Main Control Register	C10-441

C10.15	ViewInst Include-Exclude Control Register	C10-443
C10.16	ViewInst Start-Stop Control Register	C10-444
C10.17	Sequencer State Transition Control Registers 0-2	C10-445
C10.18	Sequencer Reset Control Register	C10-447
C10.19	Sequencer State Register	C10-448
C10.20	External Input Select Register	C10-449
C10.21	Counter Reload Value Registers 0-1	C10-450
C10.22	Counter Control Register 0	C10-451
C10.23	Counter Control Register 1	C10-452
C10.24	Counter Value Registers 0-1	C10-454
C10.25	ID Register 8	C10-455
C10.26	ID Register 9	C10-456
C10.27	ID Register 10	C10-457
C10.28	ID Register 11	C10-458
C10.29	ID Register 12	C10-459
C10.30	ID Register 13	C10-460
C10.31	Implementation Specific Register 0	C10-461
C10.32	ID Register 0	C10-462
C10.33	ID Register 1	C10-464
C10.34	ID Register 2	C10-465
C10.35	ID Register 3	C10-466
C10.36	ID Register 4	C10-468
C10.37	ID Register 5	C10-469
C10.38	Resource Selection Control Registers 2-16	C10-471
C10.39	Single-Shot Comparator Control Register 0	C10-472
C10.40	Single-Shot Comparator Status Register 0	C10-473
C10.41	OS Lock Access Register	C10-474
C10.42	OS Lock Status Register	C10-475
C10.43	Power Down Control Register	C10-476
C10.44	Power Down Status Register	C10-477
C10.45	Address Comparator Value Registers 0-7	C10-478
C10.46	Address Comparator Access Type Registers 0-7	C10-479
C10.47	Context ID Comparator Value Register 0	C10-481
C10.48	VMID Comparator Value Register 0	C10-482
C10.49	Context ID Comparator Control Register 0	C10-483
C10.50	Integration ATB Identification Register	C10-484
C10.51	Integration Instruction ATB Data Register	C10-485
C10.52	Integration Instruction ATB In Register	C10-486
C10.53	Integration Instruction ATB Out Register	C10-487
C10.54	Integration Mode Control Register	C10-488
C10.55	Claim Tag Set Register	C10-489
C10.56	Claim Tag Clear Register	C10-490
C10.57	Device Affinity Register 0	C10-491
C10.58	Device Affinity Register 1	C10-493
C10.59	Software Lock Access Register	C10-494
C10.60	Software Lock Status Register	C10-495
C10.61	Authentication Status Register	C10-496
C10.62	Device Architecture Register	C10-497
C10.63	Device ID Register	C10-498
C10.64	Device Type Register	C10-499

C10.65	ETM Peripheral Identification Registers	C10-500
C10.66	ETM Peripheral Identification Register 0	C10-501
C10.67	ETM Peripheral Identification Register 1	C10-502
C10.68	ETM Peripheral Identification Register 2	C10-503
C10.69	ETM Peripheral Identification Register 3	C10-504
C10.70	ETM Peripheral Identification Register 4	C10-505
C10.71	ETM Peripheral Identification Register 5-7	C10-506
C10.72	ETM Component Identification Registers	C10-507
C10.73	ETM Component Identification Register 0	C10-508
C10.74	ETM Component Identification Register 1	C10-509
C10.75	ETM Component Identification Register 2	C10-510
C10.76	ETM Component Identification Register 3	C10-511

Chapter C11

CTI registers

C11.1	Cross trigger register summary	C11-514
C11.2	External register access permissions to the CTI registers	C11-516
C11.3	CTI Device Identification Register	C11-517
C11.4	CTI Integration Mode Control Register	C11-518
C11.5	CTI Peripheral Identification Registers	C11-519
C11.6	CTI Peripheral Identification Register 0	C11-520
C11.7	CTI Peripheral Identification Register 1	C11-521
C11.8	CTI Peripheral Identification Register 2	C11-522
C11.9	CTI Peripheral Identification Register 3	C11-523
C11.10	CTI Peripheral Identification Register 4	C11-524
C11.11	CTI Peripheral Identification Register 5-7	C11-525
C11.12	CTI Component Identification Registers	C11-526
C11.13	CTI Component Identification Register 0	C11-527
C11.14	CTI Component Identification Register 1	C11-528
C11.15	CTI Component Identification Register 2	C11-529
C11.16	CTI Component Identification Register 3	C11-530

Part D

Appendices

Appendix A

Signal Descriptions

A.1	About the signal descriptions	Appx-A-534
A.2	Processor configuration signals	Appx-A-535
A.3	Clock signals	Appx-A-536
A.4	Reset signals	Appx-A-537
A.5	GIC signals	Appx-A-538
A.6	Generic Timer signals	Appx-A-541
A.7	Power management signals	Appx-A-542
A.8	L2 error signals	Appx-A-544
A.9	ACP interface signals	Appx-A-545
A.10	Broadcast signals for the memory interface	Appx-A-547
A.11	AXI interface signals	Appx-A-548
A.12	ACE interface signals	Appx-A-550
A.13	CHI interface signals	Appx-A-554
A.14	Debug signals	Appx-A-557
A.15	APB interface signals	Appx-A-559
A.16	ATB interface signals	Appx-A-560

A.17	ETM signals	Appx-A-561
A.18	PMU interface signals	Appx-A-562
A.19	CTI interface signals	Appx-A-563
A.20	DFT interface signals	Appx-A-564
A.21	MBIST interface signals	Appx-A-565

Appendix B

Revisions

B.1	Revisions	Appx-B-568
-----	-----------------	------------

Preface

This preface introduces the *ARM® Cortex-A34 Processor Technical Reference Manual*.

It contains the following:

- *About this book* on page 16.
- *Feedback* on page 20.

About this book

Cortex-A34 Technical Reference Manual. TRM. This book gives reference documentation for the Cortex-A34 processor. It contains programming details for registers and describes the memory system, caches, debug trace, and interrupts.

Product revision status

The *mpn* identifier indicates the revision status of the product described in this book, for example, *r1p2*, where:

rm Identifies the major revision of the product, for example, *r1*.

pn Identifies the minor revision or modification status of the product, for example, *p2*.

Intended audience

This manual is written for system designers, system integrators, and programmers who are designing or programming a System-on-Chip (SoC) that uses the Cortex-A34 processor.

Using this book

This book is organized into the following chapters:

Part A Functional Description

This part describes the main functionality of the Cortex-A34 processor.

Chapter A1 Introduction

This chapter provides an overview of the Cortex-A34 processor and its features.

Chapter A2 Technical Overview

This chapter describes the structure of the Cortex-A34 processor.

Chapter A3 Clocks, Resets, and Input Synchronization

This chapter describes the clocks of the Cortex-A34 processor. It also describes the reset options.

Chapter A4 Power Management

This chapter describes the power domains and the power modes in the Cortex-A34 processor.

Chapter A5 Cache Behavior and Cache Protection

This chapter describes the CPU and SCU cache protection features of the Cortex-A34 processor.

Chapter A6 L1 Memory System

This chapter describes the L1 instruction cache and data cache.

Chapter A7 L2 Memory System

This chapter describes the L2 memory system and the *Snoop Control Unit* (SCU) that is tightly integrated with it.

Chapter A8 AXI Master Interface

This chapter describes the AXI master memory interface.

Chapter A9 ACE Master Interface

This chapter describes the ACE master interface.

Chapter A10 CHI Master Interface

This chapter describes the CHI master memory interface.

Chapter A11 ACP Slave Interface

This chapter describes the ACP slave interface.

Chapter A12 GIC CPU Interface

This chapter describes the *Generic Interrupt Controller* (GIC) CPU interface of the processor.

Part B Register Descriptions

This part describes the non-debug registers of the Cortex-A34 processor.

Chapter B1 AArch64 system registers

This chapter describes the system registers in the AArch64 state.

Chapter B2 GIC registers

This chapter describes the GIC registers.

Chapter B3 Generic Timer registers

This chapter describes the Generic Timer registers.

Part C Debug

This part describes the debug functionality and registers of the Cortex-A34 processor.

Chapter C1 Debug

This chapter describes the debug features of the processor.

Chapter C2 PMU

This chapter describes the *Performance Monitor Unit* (PMU) of the processor.

Chapter C3 ETM

This chapter describes the *Embedded Trace Macrocell* (ETM) of the processor.

Chapter C4 CTI

This chapter describes the cross-trigger components of the processor.

Chapter C5 Direct access to internal memory

This chapter describes the direct access to internal memory that caches and TLBs use.

Chapter C6 Debug AArch64 registers

This chapter describes the debug registers in the AArch64 execution state and shows examples of how to use them.

Chapter C7 Debug memory mapped registers

This chapter describes the debug memory-mapped registers and shows examples of how to use them.

Chapter C8 ROM table

This section describes the ROM table that the debuggers can use to determine which components are implemented. It also describes the ROM table registers.

Chapter C9 PMU registers

This chapter describes the PMU registers.

Chapter C10 ETM registers

This chapter describes the ETM registers.

Chapter C11 CTI registers

This chapter describes the CTI registers.

Part D Appendices

Appendix A Signal Descriptions

This appendix describes the signals at the external interfaces of the processor.

Appendix B Revisions

This appendix describes the technical changes between released issues of this book.

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.

Typographic conventions

italic

Introduces special terminology, denotes cross-references, and citations.

bold

Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.

monospace

Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.

monospace

Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.

monospace italic

Denotes arguments to monospace text where the argument is to be replaced by a specific value.

monospace bold

Denotes language keywords when used outside example code.

<and>

Encloses replaceable terms for assembler syntax where they appear in code or code fragments. For example:

```
MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2>
```

SMALL CAPITALS

Used in body text for a few terms that have specific technical meanings, that are defined in the *ARM glossary*. For example, IMPLEMENTATION DEFINED, IMPLEMENTATION SPECIFIC, UNKNOWN, and UNPREDICTABLE.

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.

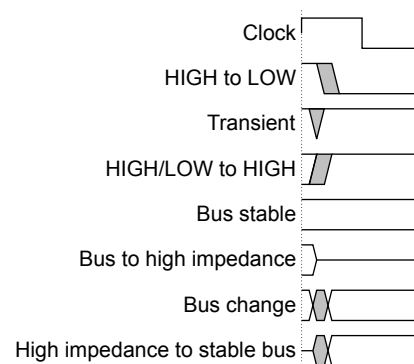


Figure 1 Key to timing diagram conventions

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 denotes an active-LOW signal.

Additional reading

This book contains information that is specific to this product. See the following documents for other relevant information.

ARM publications

- *ARM® AMBA® AXI and ACE Protocol Specification AXI, AXI4, and AXI4-Lite, ACE and ACE-Lite* (ARM IHI 0022).
- *ARM® AMBA® APB Protocol Specification* (ARM IHI 0024).
- *ARM® AMBA® ATB Protocol Specification* (ARM IHI 0032).
- *ARM® Low Power Interface Specification Q-Channel and P-Channel Interfaces* (ARM IHI 0068).
- *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* (ARM DDI 0487).
- *ARM® Generic Interrupt Controller Architecture Specification* (ARM IHI 0069).
- *ARM® Embedded Trace Macrocell Architecture Specification ETMv4* (ARM IHI 0064).
- *ARM® CoreSight™ Architecture Specification* (ARM IHI 0029).
- *ARM® Cortex-A Series Programmer's Guide for ARMv8-A* (ARM DEN 0024).

The following confidential books are only available to licensees:

- *ARM® Cortex-A34 Configuration and Sign-off Guide* (ARM 100249).
- *ARM® Cortex-A34 Processor Integration Manual* (ARM 100250).
- *ARM® Cortex-A34 Processor Cryptographic Extension Technical Reference Manual* (ARM 100247).
- *ARM® Cortex-A34 Processor Advanced SIMD and Floating-point Support Technical Reference Manual* (ARM 100248).
- *ARM® AMBA® 5 CHI Protocol Specification* (ARM IHI 0050).

Other publications

This section lists relevant documents published by third parties:

- *ANSI/IEEE Std 754-2008, IEEE Standard for Binary Floating-Point Arithmetic.*

Note

ARM floating-point terminology is largely based on the earlier ANSI/IEEE Std 754-1985 issue of the standard. See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

Feedback

Feedback on this product

If you have any comments or suggestions about this product, contact your supplier and give:

- The product name.
- The product revision or version.
- An explanation with as much information as you can provide. Include symptoms and diagnostic procedures if appropriate.

Feedback on content

If you have comments on content then send an e-mail to errata@arm.com. Give:

- The title *ARM® Cortex-A34 Processor Technical Reference Manual*.
- The number ARM 100246_0001_00_en.
- If applicable, the page number(s) to which your comments refer.
- A concise explanation of your comments.

ARM also welcomes general suggestions for additions and improvements.

————— **Note** —————

ARM tests the PDF only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the quality of the represented document when used with any other PDF reader.

Part A
Functional Description

Chapter A1

Introduction

This chapter provides an overview of the Cortex-A34 processor and its features.

It contains the following sections:

- *A1.1 About the Cortex-A34 processor on page A1-24.*
- *A1.2 Features on page A1-25.*
- *A1.3 Implementation options on page A1-26.*
- *A1.4 Supported standards and specifications on page A1-28.*
- *A1.5 Test features on page A1-29.*
- *A1.6 Design tasks on page A1-30.*
- *A1.7 Product revisions on page A1-31.*

A1.1 About the Cortex-A34 processor

The Cortex-A34 processor is a product designed to give mid-range instruction execution performance with low power consumption. It is highly configurable, allowing you to select features that are appropriate for the SoC in which it is used.

The major configuration options are:

- One to four ARMv8-A compliant cores with automatic data cache coherency.
- One shared L2 cache.
- An AXI, ACE, or CHI system bus interface.

The processor also contains:

- Logic to help with power management.
- GICv4 interrupt capability.
- A complete CoreSight subsystem to support embedded debug in each core.
- An optional ACP that allows for I/O coherent operations with an external master, for example a DMA engine.

The following figure shows an example configuration with four cores, an L2 cache, and a CHI system bus interface.

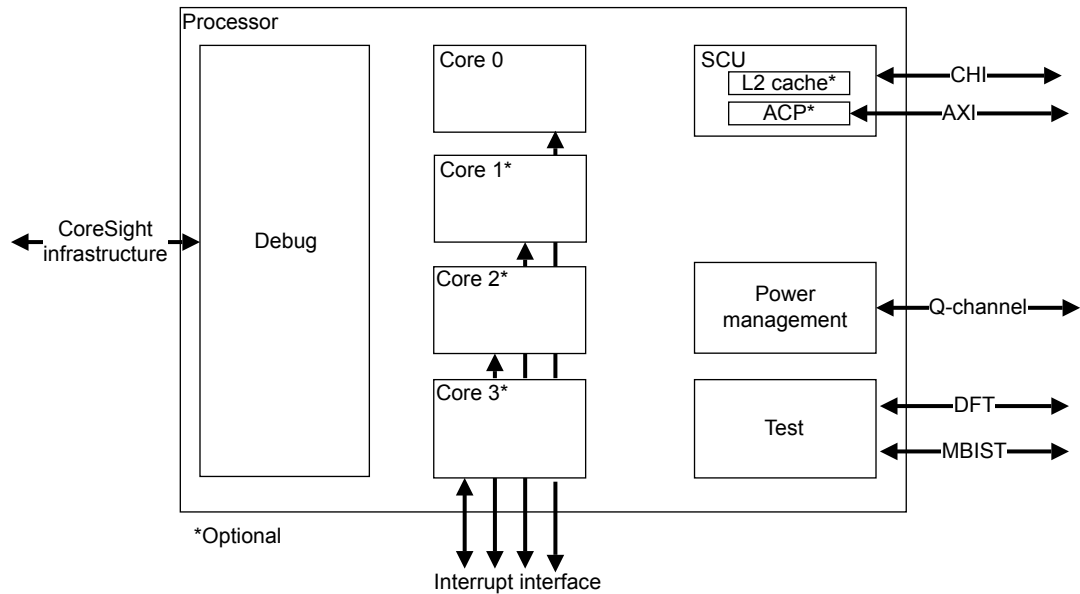


Figure A1-1 Example processor configuration

Related information

[A1.2 Features](#) on page A1-25.

[A1.3 Implementation options](#) on page A1-26.

[A1.4 Supported standards and specifications](#) on page A1-28.

[A1.5 Test features](#) on page A1-29.

[A2.1 Components](#) on page A2-34.

[A2.2 Interfaces](#) on page A2-38.

A1.2 Features

The Cortex-A34 processor includes the following features:

- Full implementation of the ARMv8-A A64 instruction set.
- The AArch64 execution state at all Exception levels (EL0 to EL3).
- In-order pipeline with direct and indirect branch prediction.
- Separate *Level 1* (L1) data and instruction side memory systems with a *Memory Management Unit* (MMU).
- *Level 2* (L2) memory system that provides cluster memory coherency.
- Optional L2 cache.
- Cache protection in the form of *Error Correction Code* (ECC) or parity on all RAM instances, except for the L2 victim RAM. There are two implementation options:
 - CPU cache protection.
 - *Snoop Control Unit* (SCU)-L2 cache protection.
- TrustZone®.
- Optional data engine that implements the Advanced SIMD and floating-point architecture support.
- Optional Cryptographic Extension. This architectural extension is only available if the data engine is present.
- ARMv8 debug logic.
- *Performance Monitoring Unit* (PMU).
- Optional *Embedded Trace Macrocell* (ETM) that supports instruction trace only.
- Optional *Generic Interrupt Controller* (GIC) CPU interface to connect to an external distributor.
- Generic Timers supporting 64-bit count input from an external system counter.

Related information

[A1.3 Implementation options on page A1-26.](#)

[A1.4 Supported standards and specifications on page A1-28.](#)

[A6.1 About the L1 memory system on page A6-82.](#)

[A7.1 About the L2 memory system on page A7-88.](#)

[A5.7 About cache protection on page A5-76.](#)

A1.3 Implementation options

The Cortex-A34 processor is highly configurable. Build-time configuration options make it possible to meet functional requirements with the smallest possible area and power. In a configuration with more than one core, all cores have the same build-time configuration.

The following table lists the implementation options for a core.

Table A1-1 Implementation options for a core

Feature	Range of options	Notes
L1 instruction cache size	<ul style="list-style-type: none"> 8K 16K 32K 64K 	
L1 data cache size	<ul style="list-style-type: none"> 8K 16K 32K 64K 	
CPU cache protection	<ul style="list-style-type: none"> Included Not included 	<ul style="list-style-type: none"> Not available if the L2 cache is implemented without SCU-L2 cache protection. Also protects the L1 duplicate tags in the SCU.
GIC CPU interface	<ul style="list-style-type: none"> Included Not included 	
ETM	<ul style="list-style-type: none"> Included Not included 	
Advanced SIMD and floating-point support	<ul style="list-style-type: none"> Included Not included 	
Cryptographic Extension	<ul style="list-style-type: none"> Included Not included 	There is no option to implement the Cryptographic Extension without the Advanced SIMD and floating-point support.

The following table lists the implementation options at build time for the processor.

Table A1-2 Implementation options for the processor

Feature	Range of options	Notes
Number of cores	<ul style="list-style-type: none"> 1 2 3 4 	All cores have the same build-time configuration.
Main bus interface	<ul style="list-style-type: none"> AMBA 4 AXI AMBA 4 ACE AMBA 5 CHI 	
L2 cache	<ul style="list-style-type: none"> Included Not included 	If it is present, all cores share one L2 cache.

Table A1-2 Implementation options for the processor (continued)

Feature	Range of options	Notes
L2 cache size	<ul style="list-style-type: none"> • 128K • 256K • 512K • 1024K 	
L2 data RAM input latency	<ul style="list-style-type: none"> • 1 cycle • 2 cycles 	
L2 data RAM output latency	<ul style="list-style-type: none"> • 2 cycles • 3 cycles 	
SCU-L2 cache protection	<ul style="list-style-type: none"> • Included • Not included 	Protects the L2 tag and L2 data RAMs with ECC.
<i>Accelerator Coherency Port (ACP)</i>	<ul style="list-style-type: none"> • Included • Not included 	Part of the SCU-L2. If the processor does not include an L2 cache, it cannot implement the ACP.
Debug memory map	<ul style="list-style-type: none"> • v8 debug memory map • v7 debug memory map 	

Related information

- [A2.2 Interfaces](#) on page A2-38.
- [A5.5 Invalidating or cleaning a cache](#) on page A5-74.
- [A6.1 About the L1 memory system](#) on page A6-82.
- [A7.1 About the L2 memory system](#) on page A7-88.
- [A5.7 About cache protection](#) on page A5-76.
- [Chapter A12 GIC CPU Interface](#) on page A12-131.
- [C1.6 Debug memory map](#) on page C1-301.
- [C3.1 About the ETM](#) on page C3-316.

A1.4 Supported standards and specifications

The Cortex-A34 processor implements the ARMv8-A architecture and some architecture extensions. It also supports various interconnect, interrupt, timer, debug, and trace architectures.

Table A1-3 Compliance with standards and specifications

Architecture specification or standard	Version	Notes
ARM architecture	ARMv8-A	<ul style="list-style-type: none"> AArch64 execution state at all Exception levels. A64 instruction set.
ARM architecture extensions	<ul style="list-style-type: none"> Advanced SIMD and floating-point support Cryptographic Extension 	<ul style="list-style-type: none"> You cannot implement floating-point without Advanced SIMD. You cannot implement the Cryptographic Extension without the Advanced SIMD and floating-point support.
Interconnect	<ul style="list-style-type: none"> AMBA 4 AXI AMBA 4 ACE AMBA 5 CHI 	You can also connect the processor to an AMBA 3 AXI interconnect.
Generic Interrupt Controller	v4	-
Generic Timer	ARMv8-A	-
PMU	v3	-
Debug	ARMv8	-
CoreSight	v2	-
Embedded Trace Macrocell	ETMv4	-

Related information

ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile.

ARM® AMBA® 5 CHI Protocol Specification.

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

ARM® Generic Interrupt Controller Architecture Specification.

ARM® CoreSight™ Architecture Specification.

ARM® ETM Architecture Specification, ETMv4.

A1.5 Test features

The Cortex-A34 processor provides test signals that enable the use of both ATPG and MBIST to test the processor and its memory arrays.

Related information

[A.20 DFT interface signals on page Appx-A-564.](#)

[A.21 MBIST interface signals on page Appx-A-565.](#)

A1.6 Design tasks

The Cortex-A34 processor is delivered as a synthesizable Register Transfer Level (RTL) description in the Verilog HDL. Before you can use it, you must implement, integrate, and program it.

A different party can perform each of the following tasks. Each task can include implementation and integration choices that affect the behavior and features of the processor.

Implementation

The implementer configures and synthesizes the RTL to produce a hard macrocell. This task includes integrating RAMs into the design.

Integration

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

Programming

It is the last task. The system programmer develops the software to configure and initialize the processor and tests the application software.

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 pre-processed. 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. The configuration choices affect the behavior of the processor.

A1.7 Product revisions

This section describes the differences in functionality between product revisions.

r0p0

First release.

r0p1

There are no functional changes in this release.

Chapter A2

Technical Overview

This chapter describes the structure of the Cortex-A34 processor.

It contains the following sections:

- *A2.1 Components* on page A2-34.
- *A2.2 Interfaces* on page A2-38.
- *A2.3 About system control* on page A2-40.
- *A2.4 About the Generic Timer* on page A2-41.
- *A2.5 About the memory model* on page A2-42.

A2.1 Components

The Cortex-A34 processor consists of:

- One to four cores, each with its own governor block. The governor block provides functionality that remains required when the core is in retention.
- An SCU-L2 memory system block. The SCU maintains data coherency between the L1 data caches and the L2 cache. It also connects the cores to an external memory system using an AXI, ACE, or CHI master interface. A mini-SCU replaces the SCU in configurations that do not require the SCU functionality. The mini-SCU is instantiated in implementations that are configured with a single core, no L2 cache, no CPU cache protection, and an AXI master interface.

The processor also integrates CoreSight components, and optionally integrates cache protection and the Cryptographic Extension.

The following figure shows a top-level functional diagram of the Cortex-A34 processor.

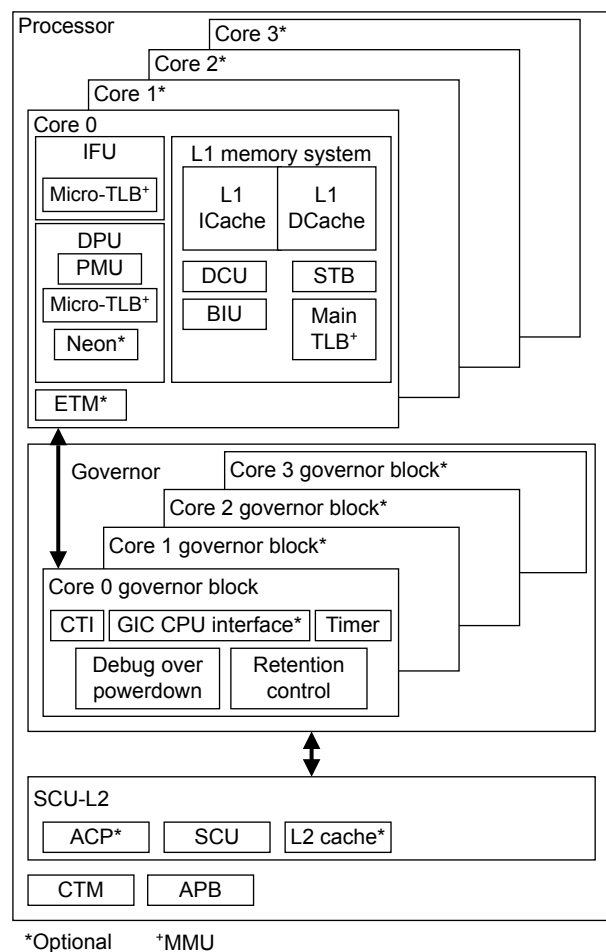


Figure A2-1 Cortex-A34 processor block diagram

Instruction Fetch Unit (IFU)

The IFU obtains instructions from the instruction cache or from external memory and predicts the outcome of branches in the instruction stream. It passes the instructions to the *Data Processing Unit* (DPU) for processing.

In implementations with CPU cache protection, parity bits protect the L1 Instruction cache data and tag RAMs by enabling the detection of any single-bit error. If an error is detected, the line is invalidated and fetched again.

Data Processing Unit (DPU)

The DPU decodes and executes instructions. It executes instructions that require data transfer to or from the memory system by interfacing to the *Data Cache Unit* (DCU). The DPU includes the *Performance Monitor Unit* (PMU), the Advanced SIMD and floating-point support, and the Cryptographic Extension.

PMU

The PMU provides six performance monitors that can be configured to gather statistics on the operation of each core and the memory system. The information can be used for debug and code profiling.

Advanced SIMD and floating-point support

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

Note

The Advanced SIMD architecture, its associated implementations, and supporting software, are also referred to as NEON technology.

Cryptographic Extension

The optional Cortex-A34 processor Cryptographic Extension supports the ARMv8 Cryptographic Extensions. It can be configured at implementation time and applies to all cores. The Cryptographic Extension adds new instructions to Advanced SIMD that accelerate:

- *Advanced Encryption Standard* (AES) encryption and decryption.
- The *Secure Hash Algorithm* (SHA) functions SHA-1, SHA-224, and SHA-256.
- Finite field arithmetic used in algorithms such as *Galois/Counter Mode* and *Elliptic Curve Cryptography*.

Memory Management Unit (MMU)

The MMU provides fine-grained memory system control through a set of virtual-to-physical address mappings and memory attributes that are held in translation tables. These are loaded into the *Translation Lookaside Buffer* (TLB) when a location is accessed. The TLB entries include global and application specific identifiers to prevent context switch TLB flushes. They also include Virtual Machine Identifiers (VMIDs) to prevent TLB flushes on virtual machine switches by the hypervisor.

Micro TLBs

The first level of caching for the translation table information is a micro TLB of ten entries. It is implemented on each of the instruction and data sides. All main TLB related maintenance operations result in flushing both the instruction and data micro TLB.

Main TLB

A unified main TLB handles misses from the micro TLBs.

In implementations with CPU cache protection, parity bits protect the TLB RAMs by enabling the detection of any single-bit error. If an error is detected, the entry is flushed and fetched again.

L1 data-side memory system

The L1 data-side memory system includes the *Data Cache Unit* (DCU), the *Store Buffer* (STB), and the *Bus Interface Unit*.

DCU

The DCU manages all load and store operations.

In implementations with CPU cache protection, parity bits protect the L1 Data cache tag RAMs and dirty RAMs. The L1 Data cache data RAMs are protected using Error Correction Codes (ECC). The ECC scheme is Single Error Correct Double Error Detect (SECCDED). The DCU includes a combined local and global exclusive monitor that is used by the Load-Exclusive/Store-Exclusive instructions.

STB

The STB holds store operations when they have left the load/store pipeline in the DCU and have been committed by the DPU. The STB can request access to the cache RAMs in the DCU, request the BIU to initiate linefills, or request the *Bus Interface Unit* (BIU) to write out the data on the external write channel. External data writes are through the SCU.

The STB is also used to queue maintenance operations before they are broadcast to other cores in the processor.

BIU

The BIU contains the SCU interface and buffers to decouple the interface from the L1 Data cache and STB. The BIU and the SCU always operate at the processor frequency.

Governor

The governor block, outside the core, includes all functions that must remain operating while a core is in retention mode.

GIC CPU interface

The GIC CPU interface is a memory-mapped interface through which a core receives an interrupt. The GIC Distributor can read and write the GIC CPU interface registers even while the core is in retention mode.

Generic timer

The Generic Timer has an interface to an external system counter. It provides a consistent view of time, which can be used to schedule events and trigger interrupts. It is also used by the retention circuits in the processor.

L2 Memory System

The L2 memory system contains the L2 cache pipeline and all the logic that maintains memory coherence between the cores in the cluster.

SCU

The SCU connects the cores to the external memory system through the master memory interface. It also maintains data cache coherency between the cores and arbitrates L2 requests from the cores.

mini-SCU

The mini-SCU replaces the SCU in certain uniprocessor configurations that do not require data cache coherency with other masters in the system. That is, implementations that are configured to have a single core, no L2 cache, no CPU cache protection, and an AXI interface. The mini-SCU bridges between the master interface of the core and the AXI master interface of the processor.

L2 cache

Each Cortex-A34 cluster can include an optional L2 cache that participates in the coherency protocol. Each L2 cache is 8-way set associative, supports 64-byte cache lines, and has a configurable cache RAM size between 128KB and 1MB.

ACP

The ACP interface cannot be configured without an L2 cache because it reuses buffering and data paths implemented for the L2 cache to achieve optimal efficiency. The main advantage of the ACP interface is its ability to allocate data in the L2 cache RAMs.

Debug and trace components

Cross-trigger

The *Cross Trigger Matrix (CTM)* combines the CoreSight *Cross Trigger Interface (CTI)* channel signals from all the cores so that a single cross trigger channel interface is presented in the Cortex-A34 processor. This module can combine up to four internal channel interfaces corresponding to each core along with one external channel interface.

Debug ROM

The Cortex-A34 processor has a debug ROM which is a CoreSight feature.

ETM

The ETM trace unit is a build-time configuration option. This module performs real-time instruction flow tracing that complies with the ETM architecture.

Related information

[A2.2 Interfaces](#) on page A2-38.

[A6.1 About the L1 memory system](#) on page A6-82.

[A7.1 About the L2 memory system](#) on page A7-88.

[Chapter A3 Clocks, Resets, and Input Synchronization](#) on page A3-43.

[Chapter A4 Power Management](#) on page A4-49.

A2.2 Interfaces

The Cortex-A34 processor has several interfaces to connect it to a SoC.

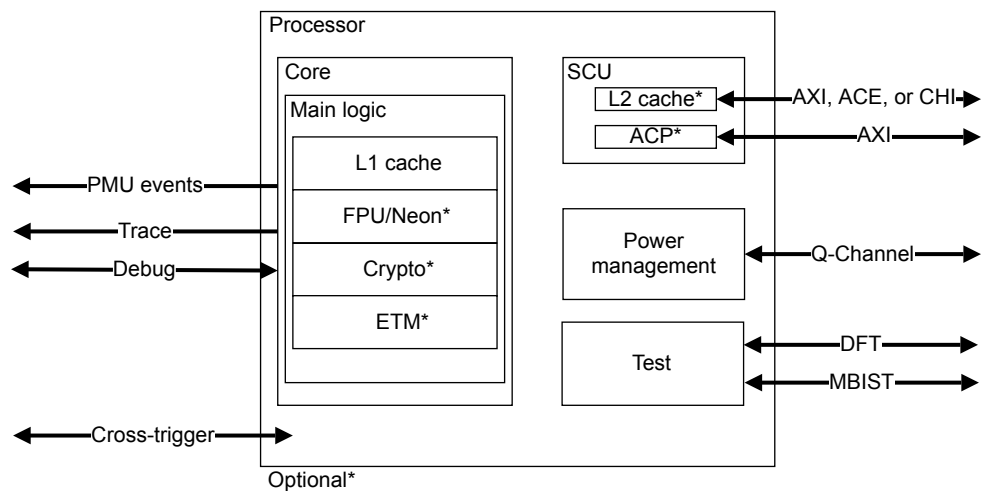


Figure A2-2 Interfaces

Table A2-1 Cortex-A34 interfaces

Purpose	Technology	Notes
PMU events		Performance events provide useful information on the operation of the processor that you can use for debug and code profiling. A subset of available performance events is exported on the PMU event bus.
Trace	ATB	Optional Outputs trace information for debugging. The ATB interface is compatible with the CoreSight architecture.
Memory	AXI, ACE, or CHI	ACE can also be used with AXI peripherals.
ACP	AXI	Optional This slave interface reduces software cache maintenance operations when the cores share memory regions with other masters and allows other masters to allocate data into the L2 cache. It allows an external master to make coherent requests to shared memory, but it does not support cache maintenance, coherency, barrier, or DVM transactions.
Debug	APB	Allows access to debug registers and resources, for example, to set watchpoints and breakpoints.
Cross-trigger	CTI	This external interface is connected to the CoreSight CTI corresponding to each core through a simplified CTM.
<i>Design for Test (DFT)</i>		Allows an industry standard <i>Automatic Test Pattern Generation (ATPG)</i> tool to test logic.
<i>Memory Built-In Self Test (MBIST)</i>		Provides support for manufacturing test of the memories embedded in the Cortex-A34 processor.
Power management	Q-channel	Enables communication to an external power controller.

Related information

[Chapter A9 ACE Master Interface on page A9-103.](#)

[Chapter A10 CHI Master Interface on page A10-115.](#)

[Chapter A8 AXI Master Interface on page A8-95.](#)

C1.2 Debug access on page C1-297.

C2.1 About the PMU on page C2-306.

C3.1 About the ETM on page C3-316.

C4.1 About the cross-trigger on page C4-324.

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, and ACE and ACE-Lite.

ARM® AMBA® 5 CHI Protocol Specification.

ARM® CoreSight™ Architecture Specification.

A2.3 About system control

The system registers control and provide status information for the functions that the processor implements.

The main functions of the system registers are:

- Overall system control and configuration.
- MMU configuration and management.
- Configuration and management of the L1 and the L2 caches.
- System performance monitoring.
- GIC configuration and management.

The system registers are accessible in the AArch64 Execution state. Some of the system registers are accessible through the memory-mapped or external debug interfaces.

Related references

[B1.1 AArch64 register summary on page B1-140.](#)

A2.4 About the Generic Timer

The Generic Timer can schedule events and trigger interrupts that are based on an incrementing counter value. It generates timer events as active-LOW interrupt outputs and event streams.

The Cortex-A34 processor does not include the system counter. This resides in the SoC. The system counter value is distributed to the Cortex-A34 processor with a synchronous binary encoded 64-bit bus, **CNTVALUEB[63:0]**.

Because **CNTVALUEB[63:0]** is generated from a system counter that typically operates at a slower frequency than the processor clock, **CLKIN**, the **CNTCLKEN** input is provided. **CNTCLKEN** is registered inside the processor and then used as a clock enable for **CNTVALUEB[63:0]**. This allows a multicycle path to be applied to the **CNTVALUEB[63:0]**. The following figure shows the interface.

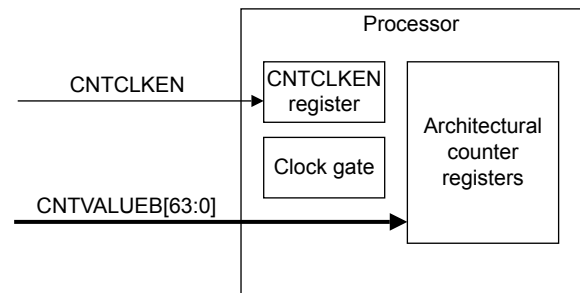


Figure A2-3 Generic Timer interface

The value on **CNTVALUEB[63:0]** is required to be stable whenever the internally registered version of the **CNTCLKEN** clock enable is asserted. **CNTCLKEN** must be synchronous and balanced with respect to **CLKIN** and must toggle at integer ratios of the processor **CLKIN**.

Related information

[A.6 Generic Timer signals on page Appx-A-541.](#)

A2.5 About the memory model

The 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 processor can store words in memory in big-endian or little-endian format. Instructions are always little-endian.

Related information

ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile.

Chapter A3

Clocks, Resets, and Input Synchronization

This chapter describes the clocks of the Cortex-A34 processor. It also describes the reset options.

It contains the following sections:

- [A3.1 Clocks on page A3-44.](#)
- [A3.2 Input synchronization on page A3-45.](#)
- [A3.3 Resets on page A3-46.](#)

A3.1 Clocks

The Cortex-A34 processor has a single clock input, **CLKIN**. All cores in the Cortex-A34 processor and the SCU are clocked with a distributed version of **CLKIN**.

The Cortex-A34 processor has the following clock enable signals:

- **PCLKENDBG.**
- **ACLKENM.**
- **ACLKENS.**
- **SCLKEN.**
- **ATCLKEN.**
- **CNTCLKEN.**

For more information, see the *ARM® Cortex-A34 Processor Integration Manual*.

A3.2 Input synchronization

The Cortex-A34 processor synchronizes certain input signals. The SoC can present these inputs asynchronously. All other external signals must be synchronous with reference to **CLKIN**.

Input signals that the Cortex-A34 processor synchronizes:

- **nCORERESET**.
- **nCPUPORESET**.
- **nFIQ**.
- **nIRQ**.
- **nL2RESET**.
- **nMBISTRESET**.
- **nPRESETDBG**.
- **nREI**.
- **nSEI**.
- **nVFIQ**.
- **nVIRQ**.
- **nVSEI**.
- **CLREXMONREQ**.
- **CPUQREQn**.
- **CTICHOUTACK**.
- **CTIIRQACK**.
- **DBGEN**.
- **EDBGRQ**.
- **EVENTI**.
- **L2FLUSHREQ**.
- **L2QREQn**.
- **NEONQREQn**.
- **NIDEN**.
- **SPIDEN**.
- **SPNIDEN**.

Input signals that the Cortex-A34 processor synchronizes under certain conditions:

- **CTICHIN**.

The synchronized **CTICHIN** input signals are used only if the **CISBYPASS** input signal is deasserted LOW. If the **CISBYPASS** signal is asserted HIGH the **CTICHIN** synchronizers are not used, and the SoC must present the **CTICHIN** synchronously to **CLKIN**.

A3.3 Resets

The Cortex-A34 processor has active-LOW reset input signals that can be asynchronously asserted HIGH to LOW, or deasserted LOW to HIGH.

nCPUPORESET[CN:0]

Where **CN** is the number of cores minus one.

Power On reset signals. These primary, cold reset signals initialize all resettable registers in the corresponding core, including debug registers and ETM registers.

nCORERESET[CN:0]

These primary reset signals initialize all resettable registers in the corresponding core, not including debug registers and ETM registers.

nPRESETDBG

This single, processor-wide signal resets the integrated CoreSight components that connect to the external **PCLK** domain, such as debug logic.

nL2RESET

This single, processor-wide signal resets all resettable registers in the L2 memory system and the logic in the SCU or mini-SCU.

nMBISTRESET

An external MBIST controller can use this signal to reset the entire SoC. The **nMBISTRESET** signal resets all resettable registers in the cluster, for entry into, and exit from, MBIST mode.

Reset synchronization logic inside the processor ensures that reset deassertion is synchronous for all resettable registers. The processor clock is not required for reset assertion, but it must be present for reset deassertion to ensure reset synchronization.

In general, the reset time only requires three processor clock cycles.

Note

The application of a retention state can affect how long reset assertion is required. You must hold the reset signal active-LOW until the power returns and the unit or processor is ready for the reset to take effect if:

- The Advanced SIMD and floating-point unit of a core undergoing a reset is in retention state.
- A core that is being reset is in retention state.

The time that is taken for retention exit and the behavior of the power controller varies by partner and by implementation.

The following table describes the valid reset signal combinations. All other combinations of reset signals are illegal. In the table, n designates the core that is reset.

Table A3-1 Valid reset combinations

Reset combination	Signals	Value	Description
Cluster cold reset	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	all = 0 all = X 0 0 1	All logic is held in reset. nCORERESET can be asserted, but is not required.
Cluster cold reset with debug active	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	all = 0 all = X 1 0 1	All cores are held in reset so they can be powered up. The L2 is held in reset, but must remain powered up. This enables external debug over power down for the cluster. nCORERESET can be asserted, but is not required.
Individual core cold reset with debug active	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	[n] = 0 [n] = X 1 1 1	Individual core is held in reset, so that the core can be powered up. This enables external debug over power down for the core that is held in reset. nCORERESET can be asserted, but is not required.
Individual core warm reset with trace and debug active	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	[n] = 1 [n] = 0 1 1 1	Individual core is held in reset.
Debug logic reset	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	all = 1 all = 1 0 1 1	Cluster debug logic is held in reset.
MBIST reset	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	all = 1 all = 1 1 1 0	All logic is held in reset.
Normal state	nCPUPORESET[CN:0] nCORERESET[CN:0] nPRESETDBG nL2RESET nMBISTRESET	all = 1 all = 1 1 1 1	No logic is held in reset.

Chapter A4

Power Management

This chapter describes the power domains and the power modes in the Cortex-A34 processor.

It contains the following sections:

- *A4.1 Power domains* on page A4-50.
- *A4.2 Power modes* on page A4-53.
- *A4.3 Core Wait for Interrupt* on page A4-54.
- *A4.4 Core Wait for Event* on page A4-55.
- *A4.5 L2 Wait for Interrupt* on page A4-56.
- *A4.6 Powering down an individual core* on page A4-57.
- *A4.7 Powering up an individual core* on page A4-58.
- *A4.8 Powering down the processor without system driven L2 flush* on page A4-59.
- *A4.9 Powering up the processor without system driven L2 flush* on page A4-60.
- *A4.10 Powering down the processor with system driven L2 flush* on page A4-61.
- *A4.11 Powering up the processor with system driven L2 flush* on page A4-62.
- *A4.12 Entering Dormant mode* on page A4-63.
- *A4.13 Exiting Dormant mode* on page A4-64.
- *A4.14 Event communication using WFE or SEV* on page A4-65.
- *A4.15 Communication to the Power Management Controller* on page A4-66.
- *A4.16 STANDBYWFI[3:0] and STANDBYWFIL2 signals* on page A4-67.
- *A4.17 Q-channel* on page A4-68.

A4.1 Power domains

A core or a processor can support different power domains. Each power domain has valid and accepted power states.

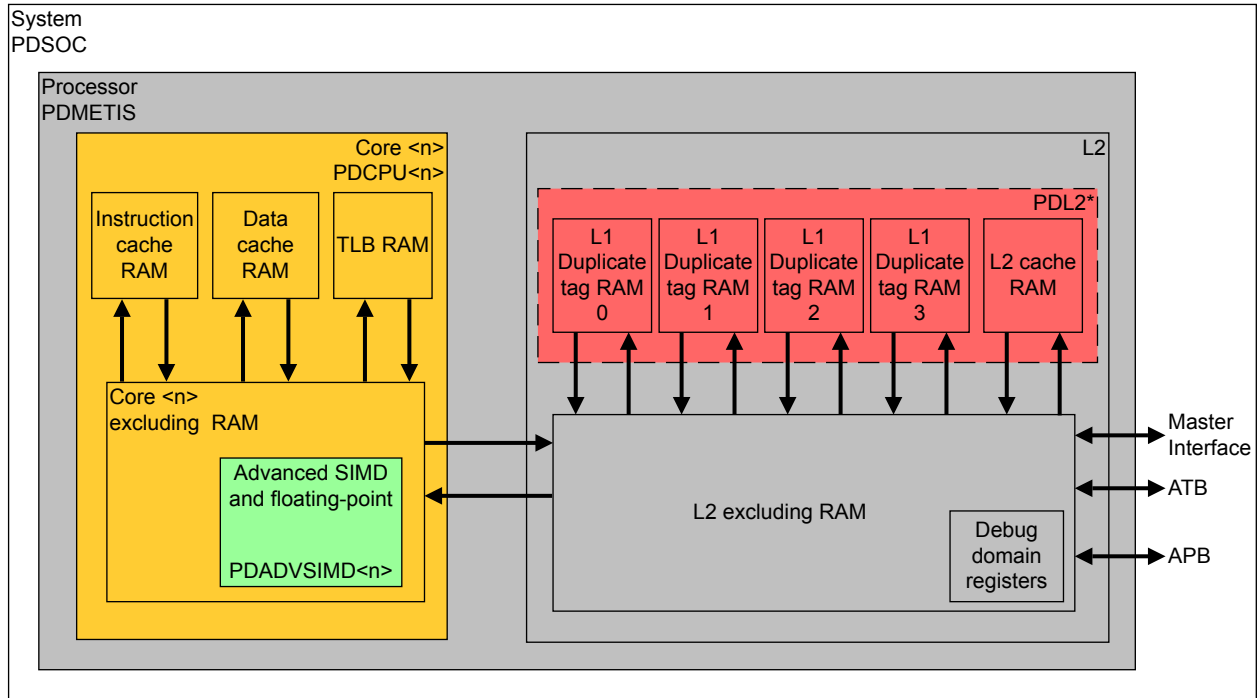
The Cortex-A34 processor provides mechanisms and support to control both dynamic and static power dissipation. The individual cores in the Cortex-A34 processor support four main levels of power management which correspond to the power domains shown in the following table:

Table A4-1 Power domain description

Power domain	Description
PDMETIS	Includes the SCU, the optional L2 cache control logic, and debug registers that are described as being in the debug domain.
PDL2	Includes the L2 data RAM, L2 tag RAM, L2 victim RAM, and the SCU duplicate tag RAM.
PDCPU<n>	Includes the optional Advanced SIMD and floating-point support, the L1 cache and TLB RAMs, and the debug registers that are described as being in the processor domain. n is 0, 1, 2, or 3. It represents core 0, core 1, core 2, or core 3. If a core is not present, the corresponding power domain is not present.
PDCPUADVSIMD<n>	Represents the Advanced SIMD and floating-point block of core n. n is 0, 1, 2, or 3. It represents core 0, core 1, core 2, or core 3. If a core is not present, the corresponding power domain is not present.

The separate PDMETIS and PDL2 power domains can remain active even when all the cores are powered down. It means that the processor can continue to accept snoops from external devices to access the L2 cache.

The following figure shows an example of the domains embedded in a *System-on-Chip* (SoC) power domain.



*If implementation includes Dormant mode support

Figure A4-1 Power domains

The power domains can be controlled independently to give different combinations of powered-up and powered-down domains. However, only some powered-up and powered-down domain combinations are valid and supported.

Table A4-2 Power state description

Power state	Description
Off	Block is power gated
Ret	Logic or RAM retention power only
On	Block is active

The following tables show the supported power domain states for the processor.

Caution

States that are not shown in the tables are unsupported and must not occur.

Table A4-3 Supported processor power states

Power domains			Description
PDMETIS	PDL2	PDCPU<n>	
Off	Off	Off	Processor off.
Off	On/Ret	Off	L2 cache dormant mode.

Table A4-3 Supported processor power states (continued)

Power domains			Description
PDMETIS	PDL2	PDCPU<n>	
On	Ret	See Table A4-4 Supported core power states on page A4-52	Processor on, L2 RAMs retained. All cores either off or in Wfx. This is an L2 RAM retention entry or residency condition.
On	Ret	See Table A4-4 Supported core power states on page A4-52	Processor on, L2 RAMs retained. At least one core running. This is a transient condition.
On	On	See Table A4-4 Supported core power states on page A4-52	Processor on, SCU/L2 RAMs active.

The following table describes the supported power domain states for individual cores. The power domain state in each core is independent of all other cores.

Table A4-4 Supported core power states

Power domains		Description
PDCPU	PDADVSIMD	
Off	Off	Core off.
On	On	Core on. Advanced SIMD and floating-point on.
On	Ret	AdvSIMD retention. Advanced SIMD and floating-point in retention.
Ret	Ret	Core retention. Core logic and Advanced SIMD and floating-point in retention.

You must follow the dynamic power management and powerup and powerdown sequences described in the following sections. Any deviation from these sequences can lead to unpredictable results.

A4.2 Power modes

The processor supports the following power modes:

Normal mode

This is the normal mode of operation in which all of the processor functionality is available. The Cortex-A34 processor uses gated clocks to disable inputs to unused functional blocks. Only the logic used to perform an operation consumes any dynamic power.

Standby mode

When a Cortex-A34 core is in standby mode, it is architecturally clock gated at the top of the clock tree. Each core in the cluster can be put in standby mode separately from the other cores, by executing a *Wait for Interrupt* (WFI) or *Wait for Event* (WFE) instruction.

L2 standby mode

When all the cores are in standby mode and the L2 memory system is idle.

Individual core shutdown mode

The PDCPU power domain for an individual core is shut down and the state held in this domain is lost.

Cluster shutdown mode

The PDMETIS, PDL2, and all PDCPU power domains are shut down and the state held in these domains is lost.

Dormant mode (optional)

All the cores and L2 control logic are powered down while the L2 cache RAMs are powered up and retain state. The RAM blocks that remain powered up during Dormant mode are:

- L2 tag RAMs.
- L2 data RAMs.
- L2 victim RAM.

Retention mode

Contact ARM for information about retention state.

A4.3 Core Wait for Interrupt

Programmers can use the *Wait for Interrupt* (WFI) instruction to cause the core to enter a low-power state.

Wait for Interrupt is a feature of the ARMv8-A architecture that puts the core in a low-power state by disabling most of the clocks in the core while keeping the core powered up. Apart from a small dynamic power overhead on the logic to enable the core to wake up from WFI low-power state, this reduces the power drawn to static leakage current only.

When executing the WFI instruction, the core waits for all instructions in the core to retire before entering the idle or low power state. The WFI instruction ensures that all explicit memory accesses that occurred before the WFI instruction in program order have retired. For example, the WFI instruction ensures that the following instructions received the required data or responses from the L2 memory system:

- Load instructions.
- Cache and TLB maintenance operations.
- Store exclusive instructions.

In addition, the WFI instruction ensures that store instructions have updated the cache or have been issued to the SCU.

While the core is in WFI low-power state, the clocks in the core are temporarily enabled without causing the core to exit WFI low-power state, when any of the following events are detected:

- A snoop request that must be serviced by the core L1 Data cache.
- A cache or TLB maintenance operation that must be serviced by the core L1 Instruction cache, data cache, or TLB.
- An APB access to the debug or trace registers residing in the core power domain.

Exit from WFI low-power state occurs when the core detects a reset or one of the WFI wake up events as described in the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

On entry into WFI low-power state, **STANDBYWFI** for that core is asserted. Assertion of **STANDBYWFI** guarantees that the core is in idle and low-power state. **STANDBYWFI** continues to assert even if the clocks in the core are temporarily enabled because of an L2 snoop request, cache or TLB maintenance operation, or an APB access.

STANDBYWFI does not indicate completion of L2 memory system transactions initiated by the processor. All Cortex-A34 processor implementations contain an L2 memory system. This includes implementations without an L2 cache.

A4.4 Core Wait for Event

A core can use the *Wait for Event* (WFE) instruction to cause the core to enter a low-power state.

Wait for Event (WFE) is a feature of the ARMv8-A architecture. It can be used by a locking mechanism based on events to put the core in a low-power state by disabling most of the clocks in the core while keeping the core powered-up. Apart from a small dynamic power overhead on the logic to enable the core to wake up from WFE low-power state, this reduces the power drawn to static leakage current only.

When executing the WFE instruction, the core waits for all instructions in the core to complete before entering the idle or low-power state.

If the event register is set, execution of a WFE instruction does not cause entry into standby state, but clears the event register.

While the core is in WFE low-power state, the clocks in the core are temporarily enabled without causing the core to exit WFE low-power state, when any of the following events are detected:

- An L2 snoop request that must be serviced by the core L1 Data cache.
- A cache or TLB maintenance operation that must be serviced by the core L1 Instruction cache, data cache, or TLB.
- An APB access to the debug or trace registers residing in the core power domain.

Exit from WFE low-power state occurs when the core detects a reset, the assertion of the **EVENTI** input signal, or one of the WFE wake-up events as described in the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

On entry into WFE low-power state, **STANDBYWFE** for that core is asserted. Assertion of **STANDBYWFE** guarantees that the core is in idle and low-power state. **STANDBYWFE** continues to assert even if the clocks in the core are temporarily enabled because of an L2 snoop request, cache or TLB maintenance operation, or an APB access.

CLREXMON request and acknowledge signaling

When the **CLREXMONREQ** input is asserted, it signals the clearing of an external global exclusive monitor and acts as a WFE wake-up event to all the cores in the cluster.

The **CLREXMONREQ** signal has a corresponding **CLREXMONACK** response signal. This forms a standard 2-wire, 4-phase handshake that can be used to signal across the voltage and frequency boundary between the core and system.

The following figure shows the **CLREXMON** request and acknowledge handshake. When the request signal is asserted, it continues to assert until an acknowledge is received. When the request is deasserted, the acknowledge can then deassert.



Figure A4-2 CLREXMON request and acknowledge handshake

A4.5 L2 Wait for Interrupt

When all the cores are in WFI low-power state, the shared L2 memory system logic that is common to all the cores can also enter a WFI low-power state.

Entry into L2 WFI low-power state can occur only if specific requirements are met and the following sequence applied:

- All cores are in WFI low-power state and therefore, the **STANDBYWFI** output for each core is asserted. Assertion of all the cores **STANDBYWFI** outputs guarantees that all the cores are in idle and low-power state. All clocks in the cores, with the exception of a small amount of clock wakeup logic, are disabled.
- If configured with ACE, the SoC asserts the input pin **ACINACTM** to idle the AXI master interface. It indicates that no snoop requests will be made from the external memory system.
- If configured with a CHI interface, the SoC asserts the input pin **SINACT** to idle the CHI master interface. It indicates that no snoop requests will be made from the external memory system.
- If configured with an ACP interface, the SoC asserts the **AINACTS** input pin to idle the ACP interface. It indicates that the SoC sends no more transactions on the ACP interface.

When the L2 memory system completes the outstanding transactions for AXI, ACE, or CHI interfaces, it can then enter the L2 WFI low-power state. On entry into L2 WFI low-power state, **STANDBYWFIL2** is asserted. Assertion of **STANDBYWFIL2** guarantees that the L2 memory system is idle and does not accept new transactions.

Exit from L2 WFI low-power state occurs on one of the following events:

- A physical IRQ or FIQ interrupt.
- A debug event.
- Powerup or warm reset.

When a core exits permanently from WFI low-power state, **STANDBYWFI** for that core is deasserted. When the L2 memory system logic exits from WFI low-power state, **STANDBYWFIL2** is deasserted. The SoC must continue to assert **ACINACTM** or **SINACT** until **STANDBYWFIL2** has deasserted.

The following figure shows the L2 WFI timing for a 4-core configuration.

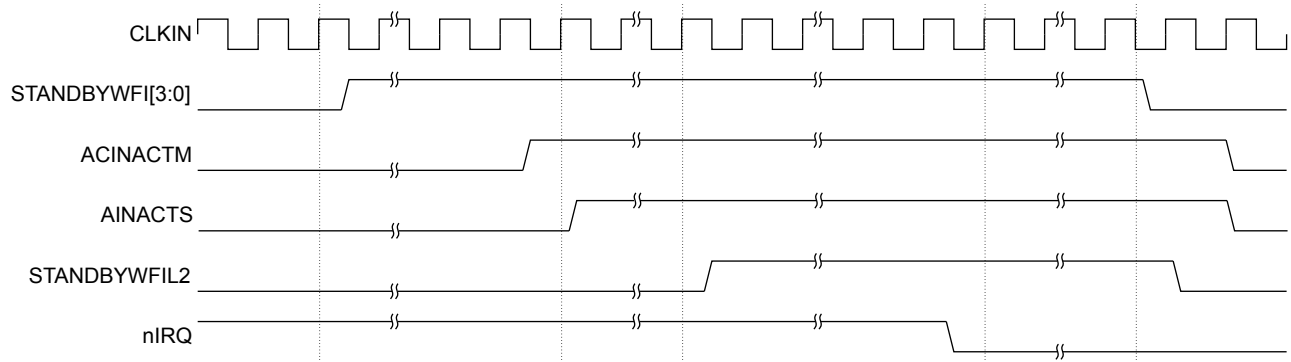


Figure A4-3 L2 Wait For Interrupt timing

A4.6 Powering down an individual core

To enable a core to be powered down, the implementation must place the core on a separately controlled power supply. In addition, you must clamp the outputs of the core to benign values while the entire cluster is powered down.

To power down the core, apply the following sequence:

Procedure

1. Disable the data cache, by clearing the SCTL.R.C bit, or the HSCTL.R.C bit if in Hyp mode. This prevents more data cache allocations and causes cacheable memory attributes to change to Normal Non-cacheable. Subsequent loads and stores do not access the L1 or L2 caches.
2. Clean and invalidate all data from the L1 Data cache. The SCU duplicate tag RAMs for this core are now empty. This prevents any new data cache snoops or data cache maintenance operations from other cores in the cluster being issued to this core.
3. Disable data coherency with other cores in the cluster, by clearing the CPUECTLR.SMPEN bit. Clearing the SMPEN bit enables the core to be taken out of coherency by preventing the core from receiving cache or TLB maintenance operations broadcast by other cores in the cluster.
4. Execute an `ISB` instruction to ensure that all of the register changes from the previous steps have been committed.
5. Execute a `DSB SY` instruction to ensure that all cache, TLB, and branch predictor maintenance operations issued by any core in the cluster device before the SMPEN bit was cleared have completed.
6. Execute a `WFI` instruction and wait until the **STANDBYWFI** output is asserted to indicate that the core is in idle and low-power state.
7. Deassert **DBGPWRDUP** LOW. This prevents any external debug access to the core.
8. Activate the core output clamps.
9. Assert **nCPUPORESET** LOW.
10. Remove power from the PDCPU power domain.

A4.7 Powering up an individual core

To power up an individual core, apply the following sequence:

1. Assert **nCPUPORESET** LOW. Ensure **DBGPWRDUP** is held LOW to prevent any external debug access to the core.
2. Apply power to the PDCPU power domain. Keep the state of the signals **nCPUPORESET** and **DBGPWRDUP** LOW.
3. Release the core output clamps.
4. Deassert resets.
5. Set the CPUECTLR.SMPEN bit to 1 to enable snooping into the core.
6. Assert **DBGPWRDUP** HIGH to allow external debug access to the core.
7. If required, use software to restore the state of the core as it was before powerdown.

A4.8 Powering down the processor without system driven L2 flush

When powering down the processor, the PDMETIS, PDL2, and PDCPU power domains are shut down and all state is lost. In this section, the lead core is defined as the last core to switch off.

To power down the processor, apply the following sequence. For device powerdown, all operations on a lead core must occur after the equivalent step on all non-lead cores.

Procedure

1. Ensure all non-lead cores are in shutdown mode, see [A4.6 Powering down an individual core on page A4-57](#).
2. Follow steps [1 on page A4-57](#) and [2 on page A4-57](#) in [A4.6 Powering down an individual core on page A4-57](#).
3. If the ACP interface is configured, ensure that any master connected to the interface does not send new transactions, then assert **AINACTS**.
4. Clean and invalidate all data from the L2 Data cache.
5. Follow steps [3 on page A4-57](#) to [10 on page A4-57](#) in [A4.6 Powering down an individual core on page A4-57](#).
6. In an ACE configuration, assert **ACINACTM** or, in a CHI configuration, assert **SINACT**. Then, wait until the **STANDBYWFIL2** output is asserted to indicate that the L2 memory system is idle. All Cortex-A34 processor implementations contain an L2 memory system, including implementations without an L2 cache. This applies to implementations that use the mini-SCU and implementations that use the SCU.
7. Activate the cluster output clamps.
8. Remove power from the PDMETIS and PDL2 power domains.

A4.9 Powering up the processor without system driven L2 flush

When powering down the processor, the PDMETIS, PDL2, and PDCPU power domains are shut down and all state is lost.

To power up the processor, apply the following sequence:

Procedure

1. For each core in the cluster, assert **nCPUPORESET** LOW.
2. Assert **nL2RESET** LOW and hold **L2RSTDISABLE** LOW.
3. Apply power to the PDMETIS and PDL2 domains while keeping the signals described in steps 1 on page A4-60 and 2 on page A4-60 LOW.
4. Release the cluster output clamps.
5. Continue a normal cold reset sequence.

A4.10 Powering down the processor with system driven L2 flush

When powering down the processor, the PDMETIS, PDL2, and PDCPU power domains are shut down and all state is lost.

To power down the cluster, apply the following sequence:

Procedure

1. Ensure all cores are in shutdown mode, see [A4.6 Powering down an individual core on page A4-57](#).
2. If the ACP interface is configured, ensure that any master connected to the interface does not send new transactions, then assert **AINACTS**. This is necessary to prevent ACP transactions from allocating new entries in the L2 cache while the hardware cache flush is occurring.
3. Assert **L2FLUSHREQ HIGH**.
4. Hold **L2FLUSHREQ HIGH** until **L2FLUSHDONE** is asserted.
5. Deassert **L2FLUSHREQ**.
6. In an ACE configuration, assert **ACINACTM** or, in a CHI configuration, assert **SINACT**. Then, wait until the **STANDBYWFIL2** output is asserted to indicate that the L2 memory system is idle. All Cortex-A34 processor implementations contain an L2 memory system, including implementations without an L2 cache. This applies to implementations that use the mini-SCU and implementations that use the SCU.
7. Activate the cluster output clamps.
8. Remove power from the PDMETIS and PDL2 power domains.

A4.11 Powering up the processor with system driven L2 flush

To power up the processor, apply the following sequence:

Procedure

1. For each core in the cluster, assert **nCPUPORESET** LOW.
2. Assert **nL2RESET** LOW and hold **L2RSTDISABLE** LOW.
3. Apply power to the PDMETIS and PDL2 domains while keeping the signals described in steps [1](#) on page A4-62 and [2](#) on page A4-62 LOW.
4. Release the cluster output clamps.
5. Continue a normal cold reset sequence.

A4.12 Entering Dormant mode

The processor can enter Dormant mode if certain requirements are met.

To support Dormant mode, you must ensure:

- That the L2 cache RAMs are in a separate power domain.
- That all inputs to the L2 cache RAMs are clamped to benign values. This avoids corrupting data when the cores and L2 control power domains enter and exit power down state.

Before entering Dormant mode, the architectural state of the cluster, excluding the contents of the L2 cache RAMs that remain powered up, must be saved to external memory.

To enter Dormant mode, apply the following sequence:

Procedure

1. Disable the data cache by clearing the SCTL.R.C bit, or the HSCTL.R.C bit if in Hyp mode. This prevents more data cache allocations and causes cacheable memory attributes to change to Normal Non-cacheable. Subsequent loads and stores do not access the L1 or L2 caches.
2. Clean and invalidate all data from the L1 Data cache. The SCU duplicate tag RAM for this core is now empty. This prevents any new data cache snoops or data cache maintenance operations from other cores in the cluster being issued to this core.
3. Disable data coherency with other cores in the cluster, by clearing the CPUECTLR.SMPEN bit. Clearing the SMPEN bit enables the core to be taken out of coherency by preventing the core from receiving cache or TLB maintenance operations broadcast by other cores in the cluster.
4. Save architectural state, if required. These state saving operations must ensure that the following occur:
 - All ARM registers, including the CPSR and SPSR, are saved.
 - All system registers are saved.
 - All debug related state is saved.
5. Execute an ISB instruction to ensure that all of the register changes from the previous steps have been committed.
6. Execute a DSB instruction to ensure that all cache, TLB, and branch predictor maintenance operations issued by any core in the cluster before the SMPEN bit was cleared have completed. In addition, this ensures that all state saving has completed.
7. Execute a WFI instruction and wait until the **STANDBYWFI** output is asserted, to indicate that the core is in idle and low-power state.
8. Repeat the previous steps for all cores, and wait for all **STANDBYWFI** outputs to be asserted.
9. If the ACP interface is configured, ensure that any master connected to the interface does not send new transactions, then assert **AINACTS**.
10. If ACE is implemented, the SoC asserts the input pin **ACINACTM** to idle the AXI master interface after all snoop transactions have been sent on the interface. If CHI is implemented, the SoC asserts the input pin **SINACT**.

When the L2 has completed the outstanding transactions for the AXI master and slave interfaces, **STANDBYWFIL2** is asserted to indicate that L2 memory system is idle. All Cortex-A34 processor implementations contain an L2 memory system, including implementations without an L2 cache.
11. When **STANDBYWFI** and **STANDBYWFIL2** are asserted for all cores, the cluster is ready to enter Dormant mode. This applies to implementations that use the mini-SCU as well as implementations that use the SCU.
12. Activate the L2 cache RAM input clamps.
13. Remove power from the PDCPU and PDMETIS power domains.

A4.13 Exiting Dormant mode

As part of the exit from Dormant mode to Normal state, the SoC must perform a cold reset sequence. The SoC must assert the reset signals until power is restored. After power is restored, the cluster exits the cold reset sequence, and the architectural state must be restored.

To exit Dormant mode, apply the following sequence:

1. Apply a normal cold reset sequence. You must apply resets to the cores and the L2 memory system logic until power is restored. During this reset sequence, **L2RSTDISABLE** must be held HIGH to disable the L2 cache hardware reset mechanism.
2. When power has been restored, release the L2 cache RAM input clamps.
3. Continue a normal cold reset sequence with **L2RSTDISABLE** held HIGH.
4. The architectural state must be restored, if required.

A4.14 Event communication using WFE or SEV

An external agent can use the **EVENTI** pin to participate in a WFE or SEV event communication with the Cortex-A34 processor.

When this pin is asserted, it sends an event message to all the cores in the device. This is similar to executing a **SEV** instruction on one core in the cluster. This enables the external agent to signal to the cores that it has released a semaphore and that the cores can leave the WFE low-power state. The **EVENTI** input pin must remain HIGH for at least one **CLKIN** clock cycle to be visible by the cores.

The external agent can determine that at least one of the cores in the cluster has executed an **SEV** instruction by checking the **EVENTO** pin. When **SEV** is executed by any of the cores in the cluster, an event is signaled to all the cores in the device, and the **EVENTO** pin is asserted. This pin is asserted HIGH for three **CLKIN** clock cycles when any core in the cluster executes an **SEV** instruction.

A4.15 Communication to the Power Management Controller

Communication between the Cortex-A34 processor and the system power management controller can be performed using one or both of the:

- [A4.16 STANDBYWFI\[3:0\] and STANDBYWFIL2 signals on page A4-67.](#)
- [A4.17 Q-channel on page A4-68.](#)

A4.16 STANDBYWFI[3:0] and STANDBYWFIL2 signals

The **STANDBYWFI[n]** signal indicates when an individual core is in idle and low-power state. The power management controller can remove power from an individual core when **STANDBYWFI[n]** is asserted.

The **STANDBYWFIL2** signal indicates when all individual cores and the L2 memory system are in idle and low-power state. A power management controller can remove power from the Cortex-A34 processor when **STANDBYWFIL2** is asserted. See [A4.8 Powering down the processor without system driven L2 flush on page A4-59](#) and [A4.10 Powering down the processor with system driven L2 flush on page A4-61](#) for more information.

The Cortex-A34 processor includes a minimal L2 memory system in configurations without an L2 cache. Therefore, the power management controller must always wait for assertion of **STANDBYWFIL2** before removing power from the Cortex-A34 processor. This applies to configurations that use the mini-SCU and configurations that use the SCU.

The following figure shows how **STANDBYWFI[3:0]** and **STANDBYWFIL2** correspond to individual cores and the Cortex-A34 processor.

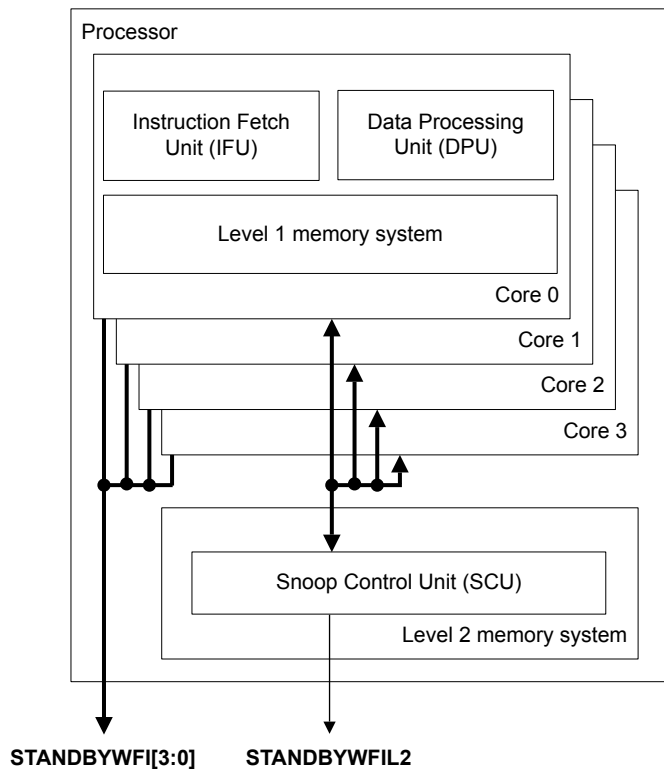


Figure A4-4 STANDBYWFI[3:0] and STANDBYWFIL2 signals

A4.17 Q-channel

Q-channel enables:

- The controller to manage entry to, and exit from, a device quiescent state. Quiescence management is typically of, but not restricted to, clock gated, and power gated retention states, of the device or device partitions.
- The capability to indicate a requirement for exit from the quiescent state. The associated signaling can contain contributions from other devices in the same power domain.
- Optional device capability to deny a quiescence request.
- Safe asynchronous interfacing across clock domains.

For more information, see the *Low Power Interface Specification: ARM Q-Channel and P-Channel Interfaces*.

Chapter A5

Cache Behavior and Cache Protection

This chapter describes the CPU and SCU cache protection features of the Cortex-A34 processor.

It contains the following sections:

- *A5.1 Cached memory types* on page A5-70.
- *A5.2 Coherency between data caches with the MOESI protocol* on page A5-71.
- *A5.3 Cache misses, unexpected cache hits, and speculative fetches* on page A5-72.
- *A5.4 Disabling a cache* on page A5-73.
- *A5.5 Invalidating or cleaning a cache* on page A5-74.
- *A5.6 About read allocate mode* on page A5-75.
- *A5.7 About cache protection* on page A5-76.
- *A5.8 Error reporting* on page A5-78.
- *A5.9 Error injection* on page A5-79.

A5.1 Cached memory types

The processor can cache data and instructions that meet certain memory attribute criteria.

L1 instruction cache

When the L1 instruction cache is enabled, it caches the following memory types:

- Normal, Inner Write-Back.
- Normal, Inner Write-Through.
- Normal, Inner Non-Cacheable.

Disabling the cache has no effect.

L1 data cache

When the L1 data cache is enabled, it can cache the following memory types:

- Normal, Inner Write-Back, Outer Write-Back.

Data might not be allocated if:

- The data is for a non-temporal load.
- The data is for a DC ZVA instruction.
- The transient hint is set.
- The no-allocate hint is set.
- The processor is in read allocate mode.

L2 cache

If the L2 cache is present and enabled, it can cache the following memory types:

- Normal, Inner Write-Back, Outer Write-Back.

Instruction cache lines are allocated into the L2 cache when they are fetched from the external memory system.

Data cache lines are allocated into the L2 cache when they are evicted from an L1 data cache.

Related information

[B1.34 CPU Auxiliary Control Register, EL1](#) on page B1-184.

A5.2 Coherency between data caches with the MOESI protocol

The processor uses the MOESI protocol to maintain data cache coherency between multiple cores. The DCU stores the MOESI state of the cache line in the tag and dirty RAMs.

MOESI describes the state in which a shareable line can be in an L1 data cache.

Table A5-1 MOESI and AMBA mapping

MOESI	AMBA	Description
Modified	UniqueDirty	The line is in only this cache and is dirty.
Owned	SharedDirty	The line is possibly in more than one cache and is dirty.
Exclusive	UniqueClean	The line is in only this cache and is clean.
Shared	SharedClean	The line is possibly in more than one cache and is clean.
Invalid	Invalid	The line is not in this cache.

Data coherency is enabled only when the CPUECTLR.SMPEN bit is set. You must set the SMPEN bit before enabling the data cache. If you do not, then the cache is not coherent with other cores and data corruption could occur.

Related information

[A5.6 About read allocate mode on page A5-75.](#)

[C5.3 Encoding for tag and data in the L1 data cache on page C5-330.](#)

A5.3 Cache misses, unexpected cache hits, and speculative fetches

The L1 and L2 caches handle problematic cache accesses in predefined ways.

Cache miss

On a cache miss, the processor performs Critical Word First filling of the cache.

Unexpected cache hits

If the cache reports a hit on a memory location that is marked as Non-Cacheable or Device, this is called an unexpected cache hit. In this architecturally UNPREDICTABLE case, the cache might return incorrect data because of the following configurations or settings:

- Improper translation table configuration because the caches are physically addressed.
- The cache is disabled.

Non-Cacheable or Device accesses do not use the result of a cache lookup and therefore ignore any unexpected cache hit.

Speculative fetches

Because there can be several unresolved branches in the pipeline, there is no guarantee that the processor executes an instruction. Instruction fetches are therefore speculative. A branch or exceptional instruction in the code stream can cause a pipeline flush and discard the fetched instructions. Because of the prefetching behavior, you must not place read-sensitive devices in the same page as code. Pages with Device memory type attributes are treated as Non-Cacheable Normal Memory when accessed by instruction fetches. You must use the XN (Execute Never) bit in the page table descriptor for a memory region to stop speculative instructions fetches when such memory region contains read-sensitive devices. To avoid speculative fetches to read-sensitive devices when address translation is disabled, these devices must be separated from code in the physical memory map.

Related information

ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile.

A5.4 Disabling a cache

Disabling the instruction cache has no effect. Fetches continue to be cached and cache maintenance operations execute normally.

When the data cache is disabled:

- Load and store instructions do not access any of the L2 or L1 data cache arrays.
- Data cache maintenance operations can still execute normally.
- All load and store instructions to cacheable memory are treated as if they were non-cacheable. It means that they are not coherent with the caches in this core or the caches in other cores and software must take account of this.

You cannot disable the L2 and L1 data caches independently because the same enable bit controls them.

Related information

[B1.71 System Control Register, EL1](#) on page B1-256.

A5.5 Invalidating or cleaning a cache

The processor automatically invalidates caches on reset unless suppressed with the **DBGL1RSTDISABLE** or **L2RSTDISABLE** pins. It is therefore not necessary for software to invalidate the caches on start-up.

DC IVAC instructions perform an invalidate of the target address. If the data is dirty within the cluster then a clean is performed before the invalidate.

DC ISW instructions perform both a clean and invalidate of the target set/way. The values of HCR.SWIO and HCR_EL2.SWIO have no effect.

The ARMv8-A architecture does not support an operation to invalidate the entire data cache. If this function is required in software, it must be constructed by iterating over the cache geometry and executing a series of individual invalidate by set/way instructions.

A5.6 About read allocate mode

The processor supports read allocate mode, also called write streaming mode, both for the L1 and the L2 cache.

Read allocate mode is a performance and power-saving optimization for writing a large block of data.

Read allocate mode for the L1 data cache

The L1 data cache supports only a Write-Back policy. It normally allocates a cache line on either a read miss or a write miss, although you can alter this by changing the inner cache allocation hints in the page tables. However, there are some situations where allocating on writes is not wanted, such as executing the C standard library `memset()` function to set a large block of memory to a known value. Writing large blocks of data like this can pollute the cache with unnecessary data. It can also waste power and reduce performance if a linefill must be performed only to discard the linefill data because the entire line was subsequently written by the `memset()` function. Therefore, the core includes logic to detect when the processor has written a full cache line before the linefill completed. If this situation is detected on a threshold number of consecutive linefills, the core switches to read allocate mode.

When the L1 data cache is in read allocate mode:

- Loads behave as normal and can still cause linefills.
- Writes still look up in the cache but if they miss, they write out to L2 rather than starting a linefill.

More than the specified number of linefills might be observed on the master interface, before the core detects that three full cache lines have been written and switches to read allocate mode.

The core continues in read allocate mode until it detects either a cacheable write burst to L2 that is not a full cache line, or there is a load to the same line as is currently being written to L2.

To configure the L1 read allocate mode threshold, use `CPUACTLR_EL1.L1RADIS`.

Read allocate mode for the L2 cache

The L2 cache enters read allocate mode after a threshold number of consecutive cache line sized writes to L2 are detected.

When the L2 cache is in read allocate mode:

- Loads behave as normal and can still cause linefills.
- Writes still lookup in the cache but if they miss, they write out to L3 rather than starting a linefill.

L2 read allocate mode continues until there is a cacheable write burst that is not a full cache line, or there is a load to the same line as is currently being written to L3.

To configure the L2 read allocate mode threshold, use `CPUACTLR_EL2.RADIS`.

Related information

[B1.34 CPU Auxiliary Control Register, EL1](#) on page B1-184.

A5.7 About cache protection

The processor protects against soft errors that result in a RAM bitcell temporarily holding the incorrect value, by writing a new value to the RAM to correct the error. If the error is a hard error that is not corrected by writing to the RAM, for example a physical defect in the RAM, then the processor might get into a livelock because it continually detects and then tries to correct the error.

Some RAMs have *Single Error Detect* (SED) capability, others have *Single Error Correct, Double Error Detect* (SECEDED) capability. The L1 data cache dirty RAM is *Single Error Detect, Single Error Correct* (SEDSEC). The processor can make progress and remain functionally correct when there is a single bit error in any RAM. If there are multiple single bit errors in different RAMs or within different protection granules within the same RAM, then the processor also remains functionally correct.

If there is a double bit error in a single RAM within the same protection granule, then the behavior depends on the RAM:

- For RAMs with SECEDED capability, the processor detects and reports the error. If the error is in a cache line that contains dirty data, that data might be lost, which then causes data corruption.
- For RAMs with only SED, the processor does not detect a double bit error. This might cause data corruption.

If there are three or more bit errors the processor might or might not detect the errors, depending on the RAM and the position of the errors within the RAM.

The cache protection feature of the processor has a minimal performance impact when no errors are present. When the processor detects an error, it stalls the access that caused the error while it corrects the error. When the correction is complete, the access either continues with the corrected data or is retried. If the access is retried, it either hits in the cache again with the corrected data or misses in the cache and re-fetches the data from a lower level cache or from main memory.

Table A5-2 Cache protection behavior of each RAM

RAM	Protection type	Configuration option	Protection granule	Correction behavior
L1 instruction cache tag	Parity, SED	CPU_CACHE_PROTECTION	30 bits	The processor invalidates both lines in the cache set then refetches the requested line from the L2 cache or external memory.
L1 instruction cache data	Parity, SED	CPU_CACHE_PROTECTION	18 bits	
TLB	Parity, SED	CPU_CACHE_PROTECTION	31 bits or 51 bits	The processor invalidates the entry and starts a new pagewalk to refetch it.
L1 data cache tag	Parity, SED	CPU_CACHE_PROTECTION	32 bits	The processor cleans the line and invalidates it from the L1 cache. It uses SCU duplicate tags to get the correct address. It refetches the line from the L2 cache or external memory.
L1 data cache data	ECC, SECEDED	CPU_CACHE_PROTECTION	32 bits	The processor cleans the line and invalidates it from the L1 cache. It corrects single bit errors as part of the eviction. It refetches the line from the L2 cache or external memory.
L1 data cache dirty	Parity, SEDSEC	CPU_CACHE_PROTECTION	1 bit	The processor cleans the line and invalidates it from the L1 cache. It corrects single bit errors as part of the eviction. Only the dirty bit is protected. The other bits are performance hints, therefore do not cause a functional failure if they are incorrect.

Table A5-2 Cache protection behavior of each RAM (continued)

RAM	Protection type	Configuration option	Protection granule	Correction behavior
SCU L1 duplicate tag	ECC, SECDED	CPU_CACHE_PROTECTION	33 bits	The processor rewrites the tag with the correct value and retries access. If the error is uncorrectable then the processor invalidates the tag.
L2 tag	ECC, SECDED	SCU_CACHE_PROTECTION	32 bits	
L2 victim	None	-	-	The victim RAM only serves as a performance hint. It does not result in a functional failure if the contents are incorrect.
L2 data	ECC, SECDED	SCU_CACHE_PROTECTION	64 bits	The processor corrects the data inline and might stall access for an additional cycle or two while the correction takes place. After correction, the processor might evict the line.

If a correctable ECC error occurs after the first data cache access of a load instruction that takes multiple cycles to complete, and if one of the following conditions has taken place:

- A hardware breakpoint, watchpoint, or vector catch has been set since the first execution that is triggered on re-execution.
- The page tables have been modified since the first execution. This resulted in an instruction or data abort trap being taken on re-execution.

then the register file is updated with data that was successfully read before the correctable ECC error occurred.

A5.8 Error reporting

The processor reports detected errors, including errors that are successfully corrected and those that cannot be corrected, in the CPUMERRSR or L2MERRSR registers. It also signals them on the **PMUEVENT** bus.

If multiple errors occur on the same clock cycle then only one of them is reported. Errors that cannot be corrected, and therefore might result in data corruption, also cause an abort or external pin to be asserted, so that software can be aware that there is an error and can either attempt to recover or can restart the system. Such errors are:

- Uncorrectable errors in the L2 data RAM when read by an instruction fetch, TLB pagewalk, or load instruction, might result in a precise data abort or prefetch abort.
- Uncorrectable errors in the L2 data RAM when read by a fetch into the L1 data cache from a load, store or preload instruction, or by the hardware prefetcher, might result in an asynchronous exception.
- Uncorrectable errors in the L1 or L2 data RAMs when the line is being evicted from a cache results in the processor asserting the **nINTERRIRQ** signal. This might be because of a natural eviction, a cache maintenance operation, or a snoop.
- Uncorrectable errors in the L2 tag RAMs or SCU L1 duplicate tag RAMs result in the processor asserting the **nINTERRIRQ** signal.
- When **nINTERRIRQ** is asserted it remains asserted until the error is cleared by a write of 0 to the L2 internal asynchronous error bit of the L2ECTLR register.
- ARM recommends that the **nINTERRIRQ** signal is connected to the interrupt controller so that an interrupt or system error is generated when the signal is asserted.

When a dirty cache line with an error on the data RAMs is evicted from the processor, the write on the master interface still takes place, however if the error is uncorrectable then:

- On AXI and ACE, the write strobes are not set, therefore the incorrect data is not written externally.
- On CHI, the strobes are set, but the response field indicates that there is a data error.

When a snoop hits on a line with an uncorrectable data error the data is returned, if required by the snoop, but the snoop response indicates that there is an error.

If a snoop hits on a tag that has an uncorrectable error, then it is treated as a snoop miss, because the error means that it is unknown if the cache line is valid or not.

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 as part of the correction process.

Related references

[B1.36 CPU Memory Error Syndrome Register, EL1](#) on page B1-189.

[B1.56 L2 Extended Control Register, EL1](#) on page B1-226.

[B1.57 L2 Memory Error Syndrome Register, EL1](#) on page B1-228.

A5.9 Error injection

To support testing of error handling software, the processor provides the capability to force double-bit errors to be injected into the L1 D-cache data RAMs, the L2 data RAMs, and the L2 tag RAMs.

Error injection on the L1 D-cache data RAMs is enabled by setting the CPUACTLR.L1DEIEN bit. While this bit is set, double-bit errors are injected on all writes to the L1 D-cache data RAMs for the first word of each 32-byte region. This corresponds to bytes with an address where bits [4:2] are 0b000. The L1 D-cache RAMs can be written to because of:

- Explicit stores from the core.
- Cache line fetches into the cache, as a result of:
 - Load instructions.
 - Store instructions.
 - Preload instructions.
 - Data prefetches.
 - Pagewalks.

Error injection on the L2 data RAMs is enabled by setting the L2ACTLR.L2DEIEN bit. While this bit is set, double-bit errors are injected on all writes to the L2 cache data RAMs. The L2 data RAMs can be written to because of:

- Explicit stores from one of the cores.
- Instruction fetches or prefetches.
- Evictions from the L1 Data cache.
- ACP accesses.

Error injection on the L2 tag RAMs is enabled by setting the L2ACTLR.L2TEIEN bit. While this bit is set, double-bit errors are injected on all writes to the L2 tag RAMs. The L2 cache tag RAMs can be written because of:

- Explicit stores from one of the cores.
- L2 allocations caused by instruction fetches or prefetches.
- Evictions from the L1 Data cache.
- ACP accesses.
- Snoop operations.
- Cache maintenance instructions.

Chapter A6

L1 Memory System

This chapter describes the L1 instruction cache and data cache.

It contains the following sections:

- *A6.1 About the L1 memory system on page A6-82.*
- *A6.2 TLB Organization on page A6-83.*
- *A6.3 Program flow prediction on page A6-84.*
- *A6.4 About the internal exclusive monitor on page A6-85.*
- *A6.5 About data prefetching on page A6-86.*

A6.1 About the L1 memory system

The L1 memory system includes several power-saving and performance-enhancing features. These include separate instruction and data caches, which can be configured independently during implementation to sizes of 8KB, 16KB, 32KB, or 64KB.

MMU

The MMU provides fine-grained memory system control through a set of virtual-to-physical address mappings and memory attributes held in translation tables. These are loaded into the *Translation Lookaside Buffer* (TLB) when a location is accessed. The key features are:

- 10-entry fully-associative instruction micro TLB.
- 10-entry fully-associative data micro TLB.
- 2-way set-associative 512-entry unified main TLB.
- 2-way set-associative 64-entry walk cache.
- 2-way set-associative 64-entry IPA cache.

L1 instruction-side memory system

The L1 instruction-side memory system provides an instruction stream to the DPU. The key features are:

- A dedicated instruction cache that:
 - is virtually indexed and physically tagged.
 - is 2-way set associative.
 - is configurable to be 8KB, 16KB, 32KB, or 64KB.
 - uses a cache line length of 64 bytes.
 - uses a pseudo-random replacement policy.
- A 128-bit read interface to the L2 memory system.
- Dynamic program flow prediction.

L1 data-side memory system

The L1 data-side memory system responds to load and store requests from the DPU. It also responds to snoop requests that have been forwarded by the SCU from other cores or external masters. The key features are:

- A dedicated data cache that:
 - is physically indexed and physically tagged.
 - is 4-way set associative.
 - is configurable to be 8KB, 16KB, 32KB, or 64KB.
 - uses a cache line length of 64 bytes.
 - uses a pseudo-random replacement policy.
- A 128-bit read and 256-bit write interface to the L2 memory system.
- A 64-bit read and 64-bit write path to the DPU.
- Read buffers that service the DCU, the IFU, and the TLB.
- Support for three outstanding data cache misses.
- Support for eight outstanding linefill requests.
- A merging store buffer.
- An internal exclusive monitor.
- An automatic data prefetch engine.
- Write stream detection and optimization (read allocate mode).

Related information

[A6.4 About the internal exclusive monitor on page A6-85.](#)

[A6.5 About data prefetching on page A6-86.](#)

[A5.6 About read allocate mode on page A5-75.](#)

A6.2 TLB Organization

This section describes the organization of the TLB.

Micro TLB

The first level of caching for the translation table information is a micro TLB of ten entries that is implemented on each of the instruction and data sides. All main TLB related maintenance operations result in flushing both the instruction and data micro TLB.

Main TLB

A unified main TLB handles misses from the micro TLBs. It has a 512-entry, 2-way, set-associative structure and supports all VMSAv8 block sizes, except 1GB. If it fetches a 1GB block, the TLB splits it into 512MB blocks and stores the appropriate block for the lookup. Accesses to the main TLB take a variable number of cycles. The number of cycles depends on the following criteria:

- Competing requests from each of the micro TLBs.
- The TLB maintenance operations in flight.
- The different page size mappings in use.

IPA cache RAM

The *Intermediate Physical Address* (IPA) cache RAM holds mappings between intermediate physical addresses and physical addresses. Only Non-secure EL1 and EL0 stage 2 translations use this cache. When a stage 2 translation is completed, it is updated and checked whenever a stage 2 translation is required.

Similarly to the main TLB, the IPA cache RAM can hold entries for different sizes.

Walk cache RAM

The walk cache RAM holds the result of a stage 1 translation up to but not including the last level. If the stage 1 translation results in a section or larger mapping then nothing is placed in the walk cache.

The walk cache holds entries fetched from Secure and Non-secure state.

A6.3 Program flow prediction

Program flow prediction is always enabled when the MMU is enabled by setting the appropriate control bit in the relevant system control register.

As a general rule, the flow prediction hardware predicts all branch outcomes regardless of the addressing mode. For example, it predicts the outcomes of the following branch types:

- Conditional branches.
- Unconditional branches.
- Indirect branches that are associated with procedure call and return instructions.

However, the flow prediction hardware does not predict the branch outcomes for the following instructions:

- Data-processing instructions that use the PC as a destination register.
- The BXJ instruction.
- Exception return instructions.

Return stack predictions

The return stack stores the return address after a procedure call type branch instruction. This address is equal to the link register value stored in X30. The following instructions cause a return stack push if predicted:

- BL.
- BLR.

In AArch64 state, the RET instruction causes a return stack pop.

Because return-from-exception instructions can change processor privilege mode and security state, they are not predicted. This includes:

- LDM (exception return)
- RFE
- SUBS pc, lr
- ERET

Related information

[B1.71 System Control Register, EL1](#) on page B1-256.

[B1.72 System Control Register, EL2](#) on page B1-259.

[B1.73 System Control Register, EL3](#) on page B1-261.

A6.4 About the internal exclusive monitor

The internal exclusive monitor is a state machine that manages Load-Exclusive or Store-Exclusive instructions, and Clear-Exclusive (CLREX) instructions. Its two states are open and exclusive.

You can use the Load-Exclusive or Store-Exclusive accesses and the Clear-Exclusive instructions to construct semaphores to ensure 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. The size of the tagged block is defined by CTR.ERG as 16 words, one cache line.

A Load-exclusive/Store-exclusive instruction is any one of the following:

- Any instruction that has a mnemonic starting with LDX, LDAX, STX, or STLX.

A Load-Exclusive instruction that causes a transaction with **ARLOCKM** for AXI/ACE, or **Excl** for CHI, set to HIGH is expected to receive an **EXOKAY** response. An **OKAY** response to a transaction with **ARLOCKM** for AXI/ACE, or **Excl** for CHI, set to HIGH indicates that exclusive accesses are not supported at the address of the transaction and causes a Data Abort exception to be taken with a Data Fault Status Code of:

- 0b110101, when using the long descriptor format.
- 0b10101, when using the short descriptor format.

A Load-Exclusive instruction causes **ARLOCKM** for AXI to be set to HIGH if the memory attributes are:

- Device.
- Normal Inner Non-cacheable and Outer Non-cacheable.
- Normal Inner is not Write-Back or Outer is not Write-Back, and Inner Shareable.
- Normal Inner is not Write-Back or Outer is not Write-Back, and Outer Shareable.

A Load-Exclusive instruction causes **ARLOCKM** for ACE or **Excl** for CHI, to be set to HIGH if the memory attributes are:

- Device.
- Normal Inner Non-cacheable and Outer Non-cacheable.
- Normal Inner Write-Back, Outer Write-Back, Outer Shareable, and **BROADCASTOUTER** is set to HIGH.
- Normal Inner Write-Back, Outer Write-Back, Inner Shareable, and **BROADCASTINNER** is set to HIGH.
- Normal Inner is not Write-Back or Outer is not Write-Back, and Inner Shareable.
- Normal Inner is not Write-Back or Outer is not Write-Back, and Outer Shareable.

In cases 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 internal exclusive monitor. The local monitor is in the Exclusive Access state after the exclusive load, remains in the Exclusive Access state after the store, and returns to the Open Access state only after the exclusive store, a CLREX instruction, or an exception return.

However, if the exclusive code sequence is accessing an address in cacheable memory, any cache line eviction that contains that address clears the monitor. ARM therefore 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.

Related references

[A8.3 AXI transactions on page A8-98.](#)

[A9.4 ACE transactions on page A9-107.](#)

[A10.5 CHI transactions on page A10-121.](#)

A6.5 About data prefetching

This section describes the software and hardware data prefetching behavior for the processor.

Preload instructions

PRFM instructions of type PLD look up in the cache and start a linefill if they miss and are to a cacheable address. These instructions retire as soon as their linefill has started, they do not wait for data to be returned. This enables other instructions to execute while the linefill continues in the background.

PRFM instructions of type PST are similar to PLD, except that if they miss, the linefill causes data to be invalidated in other cores and masters so that the line is ready for writing.

PRFM instructions also enable targeting of a prefetch to the L2 cache. When this is the case, a request is sent to the L2 memory system to start a linefill. The instruction then retires without any data being returned to the L1 memory system.

PRFM instructions of type PLI are treated as NOPs.

Automatic data prefetching and monitoring

The L1 data-side memory system implements an automatic prefetcher that monitors cache misses in the core. When a pattern is detected, the automatic prefetcher starts linefills in the background. The prefetcher recognizes a sequence of data cache misses at a fixed stride pattern that lies in four cache lines, plus or minus. Any intervening stores or loads that hit in the data cache do not interfere with the recognition of the cache miss pattern.

The CPUACTLR enables you to:

- Deactivate the prefetcher.
- Alter the sequence length required to trigger the prefetcher.
- Alter the number of outstanding requests that the prefetcher can make.

Use PRFM instructions for data prefetching where short sequences or irregular pattern fetches are required.

Non-temporal loads

Cache requests made by a non-temporal load instruction (LDNP) are allocated to the L2 cache only. The allocation policy makes it likely that the line is replaced sooner than other lines.

Data Cache Zero

The Data Cache Zero by Virtual Address (DC ZVA) instruction enables a block of 64 bytes in memory, aligned to 64 bytes in size, to be set to zero. If the DC ZVA instruction misses in the cache, it clears main memory, without causing an L1 or L2 cache allocation.

Related information

[B1.34 CPU Auxiliary Control Register, EL1 on page B1-184.](#)

Chapter A7

L2 Memory System

This chapter describes the L2 memory system and the *Snoop Control Unit* (SCU) that is tightly integrated with it.

It contains the following sections:

- *A7.1 About the L2 memory system* on page A7-88.
- *A7.2 Snoop and maintenance requests* on page A7-90.
- *A7.3 Support for memory types* on page A7-91.
- *A7.4 Memory type information exported from the processor* on page A7-92.
- *A7.5 Handling of external aborts* on page A7-93.

A7.1 About the L2 memory system

In most configurations, the L2 memory system consists of an integrated SCU that connects the cores in a cluster, an optional, tightly-coupled L2 cache, and an optional ACP interface. In single core, AXI configurations that do not include CPU cache protection, ACP, or an L2 cache, the SCU is replaced with a more area-efficient mini-SCU.

The same system register control bit enables the L1 data cache and the L2 cache.

SCU

The SCU maintains coherency between the L1 and L2 data caches in the processor. It also arbitrates requests for the L2 cache and the AXI, ACE, or CHI master interface.

A coherent request from a core is one that checks for data in the L1 data caches and, if present, the L2 cache. The SCU might send a request to another core to retrieve or invalidate data, or both, depending on the type of coherent request. This request is referred to as a snoop request. If the processor is implemented with an ACE or CHI master interface then the SCU can issue coherent requests on the master interface, which might result in snoop requests being sent to other masters in the system. The SCU might also receive snoop requests from other masters.

The SCU can handle direct cache-to-cache transfers between cores without having to read or write any data to the external memory system. Cache line migration enables dirty cache lines to be moved between cores, and there is no requirement to write back transferred cache line data to the external memory system.

Each core has tag and dirty RAMs that contain the state of the cache line in the L1 data cache. Rather than sending a snoop request to each core to access these for each coherent request, the SCU contains a set of duplicate tags that allows it to check the contents of each L1 data cache. The duplicate tags filter coherent requests so that a snoop request is only sent to a core if the coherent request hits in the corresponding duplicate tags. The duplicate tags are also used to filter snoop requests from the external memory system. This allows the cores and the system to function efficiently even with a high volume of requests.

The SCU does not support hardware management of coherency of the instruction caches. Instruction cache linefills perform coherent reads, however, there is no coherency management of data held in the instruction cache.

mini-SCU

The mini-SCU replaces the SCU in certain uniprocessor configurations that do not require data cache coherency with other masters in the system. That is, implementations that are configured to have a single CPU, no L2 cache, no CPU cache protection, and an AXI interface. The mini-SCU bridges between the master interface of the core and the AXI master interface of the processor.

L2 cache

Data cache lines are allocated to the L2 cache only when evicted from the L1 memory system, not when first fetched from the system. The only exceptions to this rule are for memory marked with the inner transient hint, or for non-temporal loads that are only ever allocated to the L2 cache. The L1 cache can prefetch data from the system, without data being evicted from the L2 cache.

Instruction cache lines are allocated to the L2 cache when fetched from the system and can be invalidated during maintenance operations.

The L2 cache is 8-way set associative. The L2 cache tags are looked up in parallel with the SCU duplicate tags. If both the L2 tag and SCU duplicate tag hit, a read accesses the L2 cache in preference to snooping one of the other cores.

L2 RAMs are invalidated automatically at reset unless the **L2RSTDISABLE** signal is set HIGH when the **nL2RESET** signal is deasserted.

Further features of the L2 cache are:

- Configurable size of 128KB, 256KB, 512KB, and 1MB.
- Fixed line length of 64 bytes.
- Physically indexed and tagged.
- Optional ECC protection.
- A pseudo-LRU replacement policy.

ACP

Optional 128-bit wide I/O coherent ACP interface that can allocate to the L2 cache.

Master memory interface

The SCU connects the cores to the external memory system through a 128-bit-wide master memory interface that uses ACE, CHI, or AXI technology. The memory interface supports integer ratios of the processor clock period up to and including 1:1 and a 40-bit physical address range.

The L2 memory system has two abort mechanisms, a synchronous one and an asynchronous one.

Related information

[A7.5 Handling of external aborts on page A7-93.](#)

[Chapter A9 ACE Master Interface on page A9-103.](#)

[Chapter A10 CHI Master Interface on page A10-115.](#)

[Chapter A8 AXI Master Interface on page A8-95.](#)

[Chapter A11 ACP Slave Interface on page A11-125.](#)

A7.2 Snoop and maintenance requests

In implementations that include an ACE or CHI master interface, the SCU controls snoop and maintenance requests to the external memory system with the **BROADCASTINNER**, **BROADCASTOUTER**, and **BROADCASTCACHEMAINT** configuration inputs.

Table A7-1 Control pins for snoop and maintenance requests

Signal	Setting	Description
BROADCASTINNER	1	The inner shareability domain extends beyond the processor. Inner Shareable snoop and maintenance operations are broadcast externally.
	0	The inner shareability domain does not extend beyond the processor.
BROADCASTOUTER	1	The outer shareability domain extends beyond the processor. Outer shareable snoop and maintenance operations are broadcast externally.
	0	The outer shareability domain does not extend beyond the processor.
BROADCASTCACHEMAINT	1	There are external downstream caches and maintenance operations are broadcast externally.
	0	There are no downstream caches external to the processor.

If you set the **BROADCASTINNER** pin to HIGH you must also set the **BROADCASTOUTER** pin to HIGH.

In a system that contains a Cortex-A34 processor and another processor in a big.LITTLE configuration, you must ensure the **BROADCASTINNER** and **BROADCASTOUTER** pins on both processors are set to HIGH so that both processors are in the same Inner Shareable domain.

Cacheable loads and stores to a shareability domain, that does not extend beyond the processor can allocate data to the L1 and L2 caches. However, they do not make coherent requests on the master for these accesses. Instead, they use only ReadNoSnoop or WriteNoSnoop transactions. This always includes non-shareable memory, and might include inner shareable and outer shareable memory, depending on the setting of the **BROADCASTINNER** and **BROADCASTOUTER** pins.

If the system sends a snoop to the Cortex-A34 processor for an address that is present in the L1 or L2 cache, but the line in the cache is in a shareability domain that does not extend beyond the cluster, then the snoop is treated as missing in the cluster.

A7.3 Support for memory types

The processor simplifies the coherency logic by downgrading some memory types.

- Memory that is marked as both Inner Write-Back Cacheable and Outer Write-Back Cacheable is cached in the L1 data cache and the L2 cache.
- Memory that is marked Inner Write-Through is downgraded to Non-cacheable.
- Memory that is marked Outer Write-Through or Outer Non-cacheable is downgraded to Non-cacheable, even if the inner attributes are Write-Back cacheable.

The attributes provided on **ARCACHE** or **AWCACHE** in AXI and ACE configurations or MemAttr and SnpAttr in CHI configurations are these downgraded attributes and indicate how the interconnect must treat the transaction.

A7.4 Memory type information exported from the processor

The processor makes attribute information about memory types available through signals for interconnects or bus protocols that require such information.

Some interconnects or bus protocols might require more information about the memory type and, for these cases, the cluster exports the memory attribute information from the translation tables stored in the TLB. These signals are for information only, and do not form part of the AXI, ACE, or CHI protocols.

- In an AXI or ACE configuration, there is a **RDMEMATTR** bus for the read channel and a **WRMEMATTR** bus for the write channel.
- In a CHI configuration, there is a single **REQMEMATTR** bus.

Table A7-2 Bus encoding for memory attributes

Bits	Encoding	Notes
[7]	Outer shareable. Always set for device memory or memory that is both inner and outer non-cacheable.	Shareability information is not recorded in the L1 data cache for implementations that use the mini-SCU. WRMEMATTR[7] is 0b0 for L1 data cache evictions in these implementations.
[6:3]	Outer memory type, or device type. If bits[1:0] indicate Device, then: 0b0000 nGnRnE. 0b0100 nGnRE. 0b1000 nGRE. 0b1100 GRE. If bits[1:0] indicate Normal, then: 0b0100 NC. 0b10RW WT. 0b11RW WB. Where R is read allocate hint, W is write allocate hint.	If an ARMv7 architecture operating system runs on the processor, the Device memory type matches the nGnRE encoding and the Strongly-Ordered memory type matches the nGnRnE memory type. Outer read allocate hint information is not recorded in the L1 or L2 data caches. WRMEMATTR[4] and REQMEMATTR[4] are set to 0b1 for data cache evictions.
[2]	Inner shareable. Anything with bit[7] set must also have bit[2] set.	Shareability information is not recorded in the L1 data cache for implementations that use the mini-SCU. WRMEMATTR[2] is 0b0 for L1 data cache evictions in these implementations.
[1:0]	Inner memory type: 0b00 Device. 0b01 NC. 0b10 WT. 0b11 WB.	

A7.5 Handling of external aborts

The memory system handles external aborts using the synchronous abort mechanism, asynchronous abort mechanism, or the **nEXTERRIRQ** pin as described in this section.

Synchronous abort mechanism

External aborts on the following accesses use the synchronous abort mechanism.

- All load accesses.
- All Store Exclusive accesses (**STREX**, **STREXB**, **STREXH**, **STREXD**, **STXR**, **STXRB**, **STXRH**, **STXP**, **STLXR**, **STLXRB**, **STLXRH**, and **STLXP**).

Asynchronous abort mechanism

External aborts on the following accesses use the asynchronous abort mechanism.

- Stores to Device memory (except Store Exclusive accesses).
- Stores to Normal memory that is Inner Non-cacheable, Inner Write-Through, Outer Non-cacheable, or Outer Write-Through (except Store Exclusive accesses).
- L1 data cache and L2 cache linefills that receive data from the interconnect in the dirty state.

nEXTERRIRQ pin

External aborts on the following accesses cause the **nEXTERRIRQ** pin to be asserted because the aborts might not relate directly back to a specific core in the cluster.

- All store accesses to Normal memory that is both Inner write-back and Outer write-back.
- Evictions from the L1 data cache or L2 cache.
- DVM Complete transactions.

Related references

[B1.56 L2 Extended Control Register, EL1](#) on page B1-226.

Chapter A8

AXI Master Interface

This chapter describes the AXI master memory interface.

It contains the following sections:

- *A8.1 About the AXI master interface* on page A8-96.
- *A8.2 AXI privilege information* on page A8-97.
- *A8.3 AXI transactions* on page A8-98.
- *A8.4 Attributes of the AXI master interface* on page A8-100.

A8.1 About the AXI master interface

You can configure the processor to use the AXI protocol for the master memory interface.

Read responses

The AXI master can delay accepting a read data channel transfer by holding **RREADY** LOW for an indeterminate number of cycles. **RREADY** can be deasserted LOW between read data channel transfers that form part of the same transaction.

Write responses

The AXI master requires that the slave does not return a write response until it has received the write address.

The AXI master always accepts write responses without delay by holding **BREADY** HIGH.

Barriers

You must ensure that your interconnect and any peripherals connected to it do not return a write response for a transaction until that transaction would be considered complete by a later barrier. This means that the write must be observable to all other masters in the system. ARM expects the majority of peripherals to meet this requirement.

Related information

[A8.2 AXI privilege information on page A8-97.](#)

A8.2 AXI privilege information

AXI provides information about the privilege level of an access on the **ARPROTM[0]** and **AWPROTM[0]** signals. However, when accesses might be cached or merged together, the resulting transaction can have both privileged and unprivileged data combined. If this happens, the processor marks the transaction as privileged, even if it was initiated by an unprivileged process.

The following table shows exception levels and corresponding **ARPROTM[0]** and **AWPROTM[0]** values.

Table A8-1 ARPROT and AWPROT values

Processor exception level	Type of access	Value of ARPROT[0] and AWPROT[0]
EL0, EL1, EL2, EL3	Cacheable read access	Privileged access
EL0	Device, or normal Non-cacheable read access	Unprivileged access
EL1, EL2, EL3		Privileged access
EL0, EL1, EL2, EL3	Cacheable write access	Privileged access
EL0	Device, nGnRnE, nGnRE, and nGRE write	Unprivileged access
EL1, EL2, EL3		Privileged access
EL0	Normal Non-cacheable or Device GRE write, except for STREX, STREXB, STREXH, STREXD, STXR, STXRB, STXRH, STXP, STLXR, STLXRB, STLXRH and STLXP to shareable memory	Privileged access
EL0	Normal Non-cacheable write for STREX, STREXB, STREXH, STREXD, STXR STXRB, STXRH, STXP, STLXR, STLXRB, STLXRH and STLXP to shareable memory	Unprivileged access
EL1, EL2, EL3	Normal Non-cacheable write	Privileged access
EL0, EL1, EL2, EL3	TLB pagewalk	Privileged access

A8.3 AXI transactions

The processor generates only a subset of all possible AXI transactions on the AXI master interface.

The processor does not generate any FIXED bursts and all WRAP bursts fetch a complete cache line starting with the critical word first. A burst does not cross a cache line boundary.

The cache linefill fetch length is always 64 bytes.

For WriteBack transfers the supported transfers are:

- WRAP 4 128-bit for read transfers (linefills).
- INCR 4 128-bit for write transfers (evictions).
- INCR N (N:1, 2, or 4) 128-bit write transfers (read allocate).

For Non-cacheable transactions:

- WRAP 4 128-bit for read transfers.
- INCR N (N:1, 2, or 4) 128-bit for write transfers.
- INCR N (N:1, 2, or 4) 128-bit for read transfers.
- INCR 1 32-bit, 64-bit, and 128-bit for read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for exclusive write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for exclusive read transfers.

For Device transactions:

- INCR N (N:1, 2, or 4) 128-bit read transfers.
- INCR N (N:1, 2, or 4) 128-bit write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-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.

For translation table walk transactions INCR 1 32-bit, and 64-bit read transfers.

The following points apply to AXI transactions:

- WRAP bursts are only 128-bit.
- INCR 1 can be any size for read or write.
- INCR burst, more than one transfer, are only 128-bit.
- No transaction is marked as FIXED.
- Write transfers with none, some, or all byte strobes LOW can occur.

External memory accesses generate the following transactions in an implementation configured with an AXI master interface.

Table A8-2 AXI transactions

Attributes		AXI transaction			
Memory type	Shareability	Load	Store	Load exclusive	Store exclusive
Device	-	Read	Write	Read with ARLOCKM set HIGH	Write with AWLOCKM set HIGH
Normal, inner Non-cacheable, outer Non-cacheable	Non-shared	Read	Write	Read	Write
	Inner-shared			Read with ARLOCKM set HIGH	Write with ARLOCKM set HIGH
	Outer-shared				

Table A8-2 AXI transactions (continued)

Attributes		AXI transaction			
Memory type	Shareability	Load	Store	Load exclusive	Store exclusive
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-shared	Read	Write	Read	Write
	Inner-shared			Read with ARLOCKM set HIGH	Write with AWLOCKM set HIGH
	Outer-shared				
Normal, inner Write-Back, outer Write-Back	Non-shared	Read	Write	Read	Write when the line is evicted
	Inner-shared				
	Outer-shared				

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

A8.4 Attributes of the AXI master interface

The table lists the possible values for the read and write issuing capabilities if the processor includes four cores.

n Number of cores.

m 1 if the processor is configured for the ACP interface, 0 if it is not.

Table A8-3 AXI master interface attributes

Attribute	Value	Comments
Write issuing capability	16	The cluster can issue a maximum of 16 writes: <ul style="list-style-type: none"> Up to 16 writes to Normal memory that is both inner and outer write-back cacheable. Up to 15 writes to all other memory types, including Device, Normal non-cacheable, and Write-through. Any mix of memory types is possible, and each write can be a single write or a write burst.
Read issuing capability	$8n + 4m$	8 for each core in the cluster including up to: <ul style="list-style-type: none"> 8 data linefills. 4 non-cacheable or Device data reads. 1 non-cacheable TLB page-walk read. 3 instruction linefills. If an ACP is configured, up to 4 ACP linefill requests can be generated.
Exclusive thread capability	n	Each core can have 1 exclusive access sequence in progress.
Write ID capability	16	The maximum number of outstanding write IDs is 16. This is the same as the maximum number of outstanding writes. 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	5	The ID encodes the source of the memory transaction. See Table A9-7 Encoding for AWIDM[4:0] on page A9-111 .
Read ID capability	$8n + 4m$	8 for each core in the processor and 4 for the ACP. 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.
Read ID width	6	The ID encodes the source of the memory transaction. See Table A9-8 Encoding for ARIDM[5:0] on page A9-111 .

In the following table, nn is the core number 0b00, 0b01, 0b10, or 0b11.

Table A8-4 Encoding for AWIDM[4:0]

Attribute	Value	Issuing capability per ID	Comments
Write ID	0b000nn	1	Core nn system domain store exclusive
	0b001xx	0	Unused
	0b010xx	0	Unused
	0b011nn	15	Core nn non-re-orderable device write
	0b1xxxx	1	Write to normal memory, or re-orderable device memory

In the following table, nn is the core number 0b00, 0b01, 0b10, or 0b11.

Table A8-5 Encoding for ARIDM[5:0]

Attribute	Value	Issuing capability per ID	Comments
Read ID	0b0000nn	4	Core nn system domain exclusive read or non-reorderable device read
	0b0001xx	0	Unused
	0b001xxx	0	Unused
	0b01xx00	1	ACP read
	0b01xx01	0	Unused
	0b01xx1x	0	Unused
	0b1xxxnn	1	Core nn read

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.

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

Chapter A9

ACE Master Interface

This chapter describes the ACE master interface.

It contains the following sections:

- *A9.1 About the ACE master interface* on page A9-104.
- *A9.2 ACE configurations* on page A9-105.
- *A9.3 ACE privilege information* on page A9-106.
- *A9.4 ACE transactions* on page A9-107.
- *A9.5 Attributes of the ACE master interface* on page A9-110.
- *A9.6 Snoop channel properties* on page A9-112.
- *A9.7 AXI compatibility mode* on page A9-113.

A9.1 About the ACE master interface

You can configure the processor to use the ACE protocol for the master memory interface.

Read responses

The ACE master can delay accepting a read data channel transfer by holding **RREADY** LOW for an indeterminate number of cycles. **RREADY** can be deasserted LOW between read data channel transfers that form part of the same transaction.

The ACE master asserts the read acknowledge signal **RACK** HIGH in the **ACLK** cycle following acceptance of the last read data channel transfer for a transaction. **RACK** is asserted in AXI compatibility mode in addition to ACE configurations.

- For interoperability of system components, ARM recommends that components interfacing with the ACE master are fully ACE compliant with no reliance on the subset of permitted **RACK** behavior described for the processor.
- If the interconnect does not perform hazarding between coherent and non-coherent requests, then, after it has returned the first transfer of read data for a non-coherent read, it must return all the remaining read transfers in the transaction, without requiring progress of any snoops to the cluster that could be to the same address.

Write responses

The ACE master requires that the slave does not return a write response until it has received the write address.

The ACE master always accepts write responses without delay by holding **BREADY** HIGH. It asserts the write acknowledge signal **WACK** HIGH in the **ACLK** cycle following acceptance of a write response. **WACK** is asserted in AXI compatibility mode in addition to ACE configurations.

For interoperability of system components, ARM recommends that components interfacing with the ACE master are fully ACE compliant with no reliance on the subset of permitted **BREADY** and **WACK** behavior described for the processor.

Barriers

The processor does not send barrier transactions to the interconnect. All barriers are terminated within the cluster.

You must ensure that your interconnect and any peripherals connected to it do not return a write response for a transaction until that transaction would be considered complete by a later barrier. This means that the write must be observable to all other masters in the system. ARM expects the majority of peripherals to meet this requirement.

Related information

[A8.2 AXI privilege information on page A8-97.](#)

A9.2 ACE configurations

This section describes the ACE configurations.

————— **Note** —————

If you want to connect the processor to an AXI interconnect, ARM recommends that you use the AXI processor configuration option. Using the ACE processor configuration option in AXI mode is less area-efficient than the AXI configuration option.

Table A9-1 Supported ACE configurations

Signal	Feature						
	AXI mode	ACE non-coherent		ACE outer coherent		ACE inner coherent	
		No L3 cache	With L3 cache	No L3 cache	With L3 cache	No L3 cache	With L3 cache
BROADCASTCACHEMAINT	0	0	1	0	1	0	1
BROADCASTOUTER	0	0	0	1	1	1	1
BROADCASTINNER	0	0	0	0	0	1	1

The following table shows the key features in each of the supported ACE configurations.

Table A9-2 Supported features in the ACE configurations

Features	Configuration				
	AXI mode	ACE non-coherent, no L3 cache	ACE non-coherent, with L3 cache	ACE outer coherent	ACE inner coherent
AXI3 or AXI4 compliance	Yes	No	No	No	No
ACE compliance	No	Yes	Yes	Yes	Yes
Barriers on AR and AW channels	No	No	No	No	No
Cache maintenance requests on AR channel	No	No	Yes	Yes	Yes
Snoops on AC channel	No	No	No	Yes	Yes
Coherent requests on AR or AW channel	No	No	No	Yes	Yes
DVM requests on AR channel	No	No	No	No	Yes

A9.3 ACE privilege information

ACE provides information about the privilege level of an access on the **ARPROTM[0]** and **AWPROTM[0]** signals. However, when accesses might be cached or merged together, the resulting transaction can have both privileged and unprivileged data combined. If this happens, the processor marks the transaction as privileged, even if it was initiated by an unprivileged process.

The following table shows exception levels and corresponding **ARPROTM[0]** and **AWPROTM[0]** values.

Table A9-3 ARPROT and AWPROT values

Processor exception level	Type of access	Value of ARPROT[0] and AWPROT[0]
EL0, EL1, EL2, EL3	Cacheable read access	Privileged access
EL0	Device, or normal Non-cacheable read access	Unprivileged access
EL1, EL2, EL3		Privileged access
EL0, EL1, EL2, EL3	Cacheable write access	Privileged access
EL0	Device, nGnRnE, nGnRE, and nGRE write	Unprivileged access
EL1, EL2, EL3		Privileged access
EL0	Normal Non-cacheable or Device GRE write, except for STREX, STREXB, STREXH, STREXD, STXR, STXRB, STXRH, STXP, STLXR, STLXRB, STLXRH, and STLXP to shareable memory	Privileged access
EL0	Normal Non-cacheable write for STREX, STREXB, STREXH, STREXD, STXR STXRB, STXRH, STXP, STLXR, STLXRB, STLXRH, and STLXP to shareable memory	Unprivileged access
EL1, EL2, EL3	Normal Non-cacheable write	Privileged access
EL0, EL1, EL2, EL3	TLB pagewalk	Privileged access

A9.4 ACE transactions

The processor generates only a subset of all possible ACE transactions on the ACE master interface.

The processor does not generate any FIXED bursts and all WRAP bursts fetch a complete cache line starting with the critical word first. A burst does not cross a cache line boundary.

The cache linefill fetch length is always 64 bytes.

For WriteBack transfers the supported transfers are:

- WRAP 4 128-bit for read transfers (linefills).
- INCR 4 128-bit for write transfers (evictions).
- INCR N (N:1, 2, or 4) 128-bit write transfers (read allocate).

For Non-cacheable transactions:

- WRAP 4 128-bit for read transfers.
- INCR N (N:1, 2, or 4) 128-bit for write transfers.
- INCR N (N:1, 2, or 4) 128-bit for read transfers.
- INCR 1 32-bit, 64-bit, and 128-bit for read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for exclusive write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit for exclusive read transfers.

For Device transactions:

- INCR N (N:1, 2, or 4) 128-bit read transfers.
- INCR N (N:1, 2, or 4) 128-bit write transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit read transfers.
- INCR 1 8-bit, 16-bit, 32-bit, 64-bit, and 128-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.

External memory accesses generate the following transactions in an implementation configured with an ACE master interface.

Table A9-4 ACE transactions

Attributes	Shareability	ACE transaction				
		Domain	Load	Store	Load exclusive	Store exclusive
Device	-	System	ReadNoSnoop	WriteNoSnoop	ReadNoSnoop and ARLOCKM set to HIGH	WriteNoSnoop and AWLOCKM set to HIGH
Normal, inner Non-cacheable, outer Non-cacheable	Non-shared	System	ReadNoSnoop	WriteNoSnoop	ReadNoSnoop and ARLOCKM set to HIGH	WriteNoSnoop and AWLOCKM set to HIGH
	Inner-shared					
	Outer-shared					

Table A9-4 ACE transactions (continued)

Attributes	ACE transaction					
	Memory type	Shareability	Domain	Load	Store	Load exclusive
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-shared	System	ReadNoSnoop	WriteNoSnoop	ReadNoSnoop	ReadNoSnoop
	Inner-shared	System	ReadNoSnoop	WriteNoSnoop	ReadNoSnoop with ARLOCKM set to HIGH	WriteNoSnoop with ARLOCKM set to HIGH
	Outer-shared	System				
Normal, inner Write-Back, outer Write-Back	Non-shared	Non-shareable	ReadNoSnoop	WriteNoSnoop	ReadNoSnoop	WriteNoSnoop
	Inner-shared	Inner Shareable	ReadShared	ReadUnique or CleanUnique if required, then a WriteBack when the line is evicted	ReadShared with ARLOCKM set to HIGH	CleanUnique with ARLOCKM set to HIGH if required, then a WriteBack when the line is evicted
	Outer-shared	Outer Shareable				

The following table shows the ACE transactions that can be generated, and some typical operations that might cause the transactions to be generated. This is not an exhaustive list of ways to generate each type of transaction, because there are many possibilities.

Table A9-5 ACE transactions and typical operations

Transaction	Operation
ReadNoSnoop	Non-cacheable loads or instruction fetches. Linefills of non-shareable cache lines into L1 or L2.
ReadOnce	Cacheable loads that are not allocating into the cache, or cacheable instruction fetches when there is no L2 cache.
ReadClean	Not used.
ReadNotSharedDirty	Not used.
ReadShared	L1 Data linefills started by a load instruction, or L2 linefills started by an instruction fetch.
ReadUnique	L1 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. Store instructions that are not allocating into the L1 or L2 caches, for example when streaming writes.
MakeUnique	Store instructions of a full cache line of data, that miss in the caches, and are allocating into the L2 cache.
CleanShared	Cache maintenance instructions.
CleanInvalid	Cache maintenance instructions.
MakeInvalid	Cache maintenance instructions.
DVM	TLB and instruction cache maintenance instructions.
DVM complete	DVM sync snoops received from the interconnect.

Table A9-5 ACE transactions and typical operations (continued)

Transaction	Operation
Barriers	DMB and DSB instructions. DVM sync snoops received from the interconnect.
WriteNoSnoop	Non-cacheable store instructions. Evictions of non-shareable cache lines from L1 and L2.
WriteUnique	Not used.
WriteLineUnique	Not used.
WriteBack	Evictions of dirty lines from the L1 or L2 cache, or streaming writes that are not allocating into the cache.
WriteClean	Evictions of dirty lines from the L2 cache, when the line is still present in an L1 cache. Some cache maintenance instructions.
WriteEvict	Evictions of unique clean lines, when configured in the L2ACTLR.
Evict	Evictions of clean lines, when configured in the L2ACTLR.

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

A9.5 Attributes of the ACE master interface

The table lists the maximum possible values for the read and write issuing capabilities if the processor includes four cores.

n Number of cores.

m 1 if the processor is configured for the ACP interface, 0 if it is not.

Table A9-6 ACE master interface attributes

Attribute	Value	Comments
Write issuing capability	16	The cluster can issue a maximum of 16 writes: <ul style="list-style-type: none"> Up to 16 writes to Normal memory that is both inner and outer write-back cacheable. Up to 15 writes to all other memory types, including Device, Normal non-cacheable, and Write-through. Any mix of memory types is possible, and each write can be a single write or a write burst.
Read issuing capability	$8n + 4m$	8 for each core in the cluster including up to: <ul style="list-style-type: none"> 8 data linefills. 4 non-cacheable or Device data reads. 1 non-cacheable TLB page-walk read. 3 instruction linefills. 5 coherency operations. 8 DVM messages. The 8 DVM messages per core can each be two-part DVM messages. They result in up to 16 DVM transactions per core. If an ACP is configured, up to 4 ACP linefill requests can be generated.
Exclusive thread capability	n	Each core can have 1 exclusive access sequence in progress.
Write ID capability	16	The maximum number of outstanding write IDs is 16. This is the same as the maximum number of outstanding writes. 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	5	The ID encodes the source of the memory transaction. See Table A9-7 Encoding for AWIDM[4:0] on page A9-111 .
Read ID capability	$8n + 4m$	8 for each core in the processor and 4 for the ACP. 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. Two part DVMs use the same ID for both parts, and therefore can have two outstanding transactions on the same ID.
Read ID width	6	The ID encodes the source of the memory transaction. See Table A9-8 Encoding for ARIDM[5:0] on page A9-111 .

In the following table, nn is the core number 0b00, 0b01, 0b10, or 0b11.

Table A9-7 Encoding for AWIDM[4:0]

Attribute	Value	Issuing capability per ID	Comments
Write ID	0b000nn	1	Core nn system domain store exclusive
	0b001xx	0	Unused
	0b010xx	0	Unused
	0b011nn	15	Core nn non-re-orderable device write
	0b1xxxx	1	Write to normal memory, or re-orderable device memory

In the following table, nn is the core number 0b00, 0b01, 0b10, or 0b11.

Table A9-8 Encoding for ARIDM[5:0]

Attribute	Value	Issuing capability per ID	Comments
Read ID	0b0000nn	4	Core nn exclusive read or non-reorderable device read
	0b0001xx	0	Unused
	0b001000	0	Unused
	0b001001	1	DVM complete
	0b00101x	0	Unused
	0b0011xx	0	Unused
	0b01xx00	1	ACP read
	0b01xx01	0	Unused
	0b01xx1x	0	Unused
	0b1xxxnn	1	Core nn read

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.

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

A9.6 Snoop channel properties

The table shows the properties of the ACE channels.

Table A9-9 ACE channel properties

Property	Value	Comment
Snoop acceptance capability	8	The SCU can accept and process a maximum of eight snoop requests from the system. It counts requests from the request being accepted on the AC channel to the response being accepted on the CR channel.
Snoop latency	Hit	When there is a hit in L2 cache, the best case for response and data is 13 processor cycles. When there is a miss in L2 cache and a hit in L1 cache, the best case for response and data is 16 processor cycles. Latencies can be higher if hazards occur or if there are not enough buffers to absorb requests.
	Miss	Best case six processor cycles when the SCU duplicate tags and L2 tags indicate the miss.
	DVM	The cluster takes a minimum of six cycles to provide a response to DVM packets.
Snoop filter	Supported	<p>The cluster provides support for an external snoop filter in an interconnect. It indicates when clean lines are evicted from the processor by sending Evict transactions on the write channel.</p> <p>However there are some cases where incorrect software can prevent an Evict transaction from being sent. Therefore you must ensure that you build any external snoop filter to handle a capacity overflow that sends a back-invalidation to the processor if it runs out of storage.</p> <p>Examples of cases where evicts are not produced include:</p> <ul style="list-style-type: none"> • Linefills that take external aborts. • Store exclusives that fail. • Mismatched aliases.
Supported transactions	-	<p>All transactions described by the ACE protocols:</p> <ul style="list-style-type: none"> • Are accepted on the master interface from the system. • Can be produced on the ACE master interface except: <ul style="list-style-type: none"> — WriteUnique. — WriteLineUnique. — ReadNotSharedDirty. — ReadClean.

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, ACE and ACE-Lite.

A9.7 AXI compatibility mode

The processor implements an AXI3/AXI4 compatibility mode in ACE configurations. With this mode you can use the processor in a standalone environment where the AMBA 4 ACE interface is not required.

To enable the AXI compatibility mode, you must ensure that the **BROADCASTINNER**, **BROADCASTOUTER**, and **BROADCASTCACHEMAIN** input pins are set to LOW.

————— **Note** —————

The AXI build-time configuration option provides a more area-efficient AXI solution than the AXI compatibility mode in ACE configurations.

Chapter A10

CHI Master Interface

This chapter describes the CHI master memory interface.

It contains the following sections:

- *A10.1 About the CHI master interface* on page A10-116.
- *A10.2 CHI configurations* on page A10-117.
- *A10.3 Attributes of the CHI master interface* on page A10-118.
- *A10.4 CHI channel properties* on page A10-120.
- *A10.5 CHI transactions* on page A10-121.

A10.1 About the CHI master interface

You can configure the processor to use the CHI protocol for the master memory interface.

A10.2 CHI configurations

This section describes the CHI configurations.

The following table shows the permitted combinations of these signals and the supported configurations in the Cortex-A34 processor, with a CHI bus.

Table A10-1 Supported CHI configurations

Signal	Feature					
	CHI non-coherent		CHI outer coherent		CHI inner coherent	
	No L3 cache	With L3 cache	No L3 cache	With L3 cache	No L3 cache	With L3 cache
BROADCASTCACHEMAINT	0	1	0	1	0	1
BROADCASTOUTER	0	0	1	1	1	1
BROADCASTINNER	0	0	0	0	1	1

The following table shows the key features in each of the supported CHI configurations.

Table A10-2 Supported features in the CHI configurations

Features	Configuration			
	CHI non-coherent, no L3 cache	CHI non-coherent, with L3 cache	CHI outer coherent	CHI inner coherent
Cache maintenance requests on TXREQ channel	No	Yes	Yes	Yes
Snoops on RXREQ channel	No	No	Yes	Yes
Coherent requests on TXREQ channel	No	No	Yes	Yes
DVM requests on TXREQ channel	No	No	No	Yes

A10.3 Attributes of the CHI master interface

The table lists the possible values for the read and write issuing capabilities if the processor includes four cores.

- n** Number of cores.
- m** 1 if the processor is configured for the ACP interface, 0 if it is not.
- w** (write issuing capability)+1.

Table A10-3 Attributes of the CHI master memory interface

Attribute	Value	Comments
Write issuing capability	Configuration dependent	<p>The maximum number of writes varies, depending on the configuration of the processor:</p> <ul style="list-style-type: none"> • The number of cores. • The presence of the L2 cache. <p>If no L2 cache is configured:</p> <p>One core 5 outstanding writes. 2-4 cores 8 outstanding writes.</p> <p>If an L2 cache is configured:</p> <p>One core 7 outstanding writes. 2-4 cores 10 outstanding write.</p> <p>A cluster with four cores, with L2 cache, can issue 10 outstanding transactions. A processor with one core, without L2 cache, can issue five outstanding transactions.</p> <p>All outstanding transactions use a unique ID.</p>
Read issuing capability	$8n + 4m + 1$	<p>8 for each core in the cluster including up to:</p> <ul style="list-style-type: none"> • 8 data linefills. • 4 Non-cacheable or Device data reads. • 1 Non-cacheable TLB page-walk read. • 3 instruction linefills. • 5 coherency operations. • 1 barrier operation. • 8 DVM messages. <p>If an ACP is configured, up to 4 ACP linefill requests can be generated. 1 barrier operation is generated from the cluster.</p>
Exclusive thread capability	n	Each core can have 1 exclusive access sequence in progress.
Transaction ID width	8	The ID encodes the source of the memory transaction. See A9.5 Attributes of the ACE master interface on page A9-110.
Transaction ID capability	$8n + 4m + w + 1$	<p>8 for each core in the cluster in addition to:</p> <ul style="list-style-type: none"> • 4 for the ACP interface. • 1 for barriers. • 6 to 11 writes, depending on the write issuing capability. <p>Unlike in configurations with AXI or ACE, there is never any ID reuse in CHI implementations, regardless of the memory type.</p>

There is no fixed mapping between CHI transaction IDs and cores. Some transaction IDs can be used for either reads or writes.

Related information

A9.5 Attributes of the ACE master interface on page A9-110.

ARM® AMBA® 5 CHI Protocol Specification.

A10.4 CHI channel properties

You can configure the processor to use the CHI protocol for the master memory interface

Table A10-4 CHI channel properties

Property	Value	Comment
Snoop acceptance capability	10	The SCU can accept and process a maximum of 10 snoop requests from the system.
DVM acceptance capability	4	The SCU can accept and process a maximum of four DVM transactions from the system. Each of these four transactions can be a two part DVM message. The interconnect must be configured to never send more than four DVM messages to a Cortex-A34 processor, otherwise the system might deadlock.
Snoop latency	Hit	When there is a hit in L2 cache, the best case for response and data is 11 processor cycles. When there is a miss in L2 cache and a hit in L1 cache, the best case for response and data is 14 processor cycles. Latencies can be higher if hazards occur or if there are not enough buffers to absorb requests.
	Miss	Best case six processor cycles when the SCU duplicate tags and L2 tags indicate the miss.
	DVM	The cluster takes a minimum of six 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 processor by sending Evict transactions on the CHI write channel. However, there are some cases where incorrect software can prevent an Evict transaction from being sent, therefore you must ensure that any external snoop filter is built to handle a capacity overflow that sends a back-invalidation to the processor if it runs out of storage.
Supported transactions	-	All transactions described by the CHI protocol: <ul style="list-style-type: none"> • Are accepted on the CHI master interface from the system. • Can be produced on the CHI master interface except: <ul style="list-style-type: none"> — ReadClean. — WriteBackPtl. — WriteCleanPtl.

Related information

[ARM® AMBA® 5 CHI Protocol Specification.](#)

A10.5 CHI transactions

CHI transactions are sent to a specific node in the interconnect 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 page 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.

Table A10-5 CHI transaction IDs

Transaction ID	Description
000nnxxx	Transaction from core nn. Can be a: <ul style="list-style-type: none"> • Read transaction. • Write transaction. • Cache maintenance transaction. • DVM transaction. • Barrier transaction.
001001xx	Transaction from the ACP interface. Can be a read or write.
00101110	Barrier generated in response to a DVM sync snoop from the interconnect.
0100xxxx	Eviction from L1 or L2 cache. The number of IDs used depends on the configuration.

Table A10-6 CHI transactions

Transaction	Operation
ReadNoSnp	Non-cacheable loads or instruction fetches. Linefills of non-shareable cache lines into L1 or L2.
ReadOnce	Cacheable loads that are not allocating into the cache, or cacheable instruction fetches when there is no L2 cache.
ReadClean	Not used.
ReadShared	L1 Data linefills started by a load instruction, or L2 linefills started by an instruction fetch.
ReadUnique	L1 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, and are allocating into the L2 cache.
CleanShared	Cache maintenance instructions.
CleanInvalid	Cache maintenance instructions.
MakeInvalid	Cache maintenance instructions.
DVMOp	TLB and instruction cache maintenance instructions.
EOBarrier	DMB instructions.
ECBarrier	DSB instructions. DVM sync snoops received from the interconnect.
WriteNoSnpPtl	Non-cacheable store instructions.
WriteNoSnpFull	Non-cacheable store instructions, or evictions of non-shareable cache lines from the L1 and L2 cache.
WriteUniqueFull	Cacheable writes of a full cache line, that are not allocating into L1 or L2 caches, for example streaming writes.
WriteUniquePtl	Cacheable writes of less than a full cache line that are not allocating into L1 or L2.

Table A10-6 CHI transactions (continued)

Transaction	Operation
WriteBackFull	Evictions of dirty lines from the L1 or L2 cache.
WriteBackPtl	Not used.
WriteCleanFull	Evictions of dirty lines from the L2 cache, when the line is still present in an L1 cache. Some cache maintenance instructions.
WriteCleanPtl	Not used.
WriteEvictFull	Evictions of unique clean lines, when configured in the L2ACTLR.
Evict	Evictions of clean lines, when configured in the L2ACTLR.

External memory accesses generate the following transactions in an implementation configured with a CHI master interface.

Table A10-7 CHI transactions

Attributes	CHI transaction					
	Shareability	SnpAttr	Load	Store	Load exclusive	Store exclusive
Device	-	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp and Excl set to HIGH	WriteNoSnp and Excl set to HIGH
Normal, inner Non-cacheable, outer Non-cacheable	Non-shared	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp and Excl set to HIGH	WriteNoSnp and Excl set to HIGH
	Inner-shared					
	Outer-shared					
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-shared	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp	ReadNoSnp
	Inner-shared	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp with Excl set to HIGH	WriteNoSnp with Excl set to HIGH
	Outer-shared	Non-snoopable				

Table A10-7 CHI transactions (continued)

Attributes	CHI transaction					
Memory type	Shareability	SnpAttr	Load	Store	Load exclusive	Store exclusive
Normal, inner Write-Back, outer Write-Back	Non-shared	Non-snoopable	ReadNoSnp	WriteNoSnp	ReadNoSnp	WriteNoSnp
	Inner-shared	Inner snoopable	ReadShared	ReadUnique, CleanUnique, or MakeUnique if allocating into the cache, then a WriteBackFull when the line is evicted. WriteUniqueFull or WriteUniquePtl if not allocating into the cache.	ReadShared with Excl set to HIGH	CleanUnique with Excl set to HIGH if required, then a WriteBackFull when the line is evicted
	Outer-shared	Outer snoopable				

Related information

ARM® AMBA® 5 CHI Protocol Specification.

Chapter A11

ACP Slave Interface

This chapter describes the ACP slave interface.

It contains the following sections:

- *A11.1 About the ACP* on page A11-126.
- *A11.2 Transfer size support* on page A11-127.
- *A11.3 ACP performance* on page A11-128.
- *A11.4 ACP user signals* on page A11-129.

A11.1 About the ACP

The optional *Accelerator Coherency Port (ACP)* is implemented as an AXI4 slave interface with some restrictions.

- 128-bit read and write interfaces.
- **ARCACHE** and **AWCACHE** are restricted to Normal, Write-Back, Read-Write-Allocate, Read-Allocate, Write-Allocate, and No-Allocate memory. **ARCACHE** and **AWCACHE** are limited to the values **0b0111**, **0b1011**, and **0b1111**. Other values cause a SLVERR response on **RRESP** or **BRESP**.
- Exclusive accesses are not supported.
- Barriers are not supported. The **BRESP** handshake for a write transaction indicates global observability for that write.
- **ARSIZE** and **AWSIZE** signals are not present and assume a value of **0b100**, 16 bytes.
- **ARBURST** and **AWBURST** signals are not present and assume a value of INCR.
- **ARLOCK** and **AWLOCK** signals are not present.
- **ARQOS** and **AWQOS** signals are not present.
- **ARLEN** and **AWLEN** are limited to values 0 and 3.

A11.2 Transfer size support

ACP supports the following read-request transfer size and length combinations:

- 64 byte INCR request characterized by:
 - **ARLEN** is 0x03, 4 beats.
 - **ARADDR** aligned to 64 byte boundary, so **ARADDR[5:0]** is 0b00 0000.
 - **ARSIZE** and **ARBURST** assume values of 0b100 and INCR respectively.
- 16 byte INCR request characterized by:
 - **ARLEN** is 0x00, 1 beat.
 - **ARADDR** aligned to 16 byte boundary, so **ARADDR[3:0]** is 0x0.

ACP supports the following write-request transfer size and length combinations:

- 64 byte INCR request characterized by:
 - **AWLEN** is 0x03, 4 beats.
 - **AWADDR** aligned to 64 byte boundary, so **AWADDR[5:0]** is 0b00 0000.
 - **AWSIZE** and **AWBURST** assume values of 0b100 and INCR respectively.
 - **WSTRB** for all beats must be the same and either all asserted or all deasserted.
- 16 byte INCR request characterized by:
 - **AWLEN** is 0x00, 1 beat.
 - **AWADDR** aligned to 16 byte boundary, so **AWADDR[3:0]** is 0x0.
 - **AWSIZE** and **AWBURST** assume values of 0b100 and INCR respectively.
 - **WSTRB** can take any value.

Requests not meeting these restrictions cause a SLVERR response on **RRESP** or **BRESP**.

A11.3 ACP performance

The ACP interface can support up to four outstanding transactions. These can be any combination of reads and writes.

The master must avoid sending more than one outstanding transaction on the same AXI ID, to prevent the second transaction stalling the interface until the first has completed. If the master requires explicit ordering between two transactions, ARM recommends that it waits for the response to the first transaction before sending the second transaction.

Writes are higher performance when they contain a full cache line of data.

If SCU cache protection is configured, writes of less than 64 bits incur an overhead of performing a read-modify-write sequence if they hit in the L2 cache.

Some L2 resources are shared between the ACP interface and the cores, therefore heavy traffic on the ACP interface might, in some cases, reduce the performance of the cores.

AXI and ACE You can use the **ARCACHE** and **AWCACHE** signals to control whether the ACP request causes an allocation into the L2 cache if it misses.

CHI To ensure correct ordering of data beats, ACP reads that miss always allocate into the L2 cache.

A11.4 ACP user signals

ACP transactions can cause coherent requests to the system. Therefore ACP requests must pass Inner and Outer Shareable attributes to the L2. Use specific encoding to pass the shareability attribute.

Table A11-1 Encoding of the ACP shareability attribute

AxUSER[1:0]	Attribute
0b00	Non-shareable
0b01	Inner Shareable
0b10	Outer Shareable

This is the same encoding as **AxDOMAIN** on ACE, except that a value of 0b11 is not supported.

Chapter A12

GIC CPU Interface

This chapter describes the *Generic Interrupt Controller* (GIC) CPU interface of the processor.

It contains the following sections:

- *A12.1 Bypassing the GIC CPU Interface* on page A12-132.
- *A12.2 Memory map for the GIC CPU interface* on page A12-133.

A12.1 Bypassing the GIC CPU Interface

The processor optionally implements the GIC CPU Interface. If present, you can disable it by asserting the **GICCDISABLE** signal HIGH at reset.

If the GIC is enabled, the input pins **nVIRQ** and **nVFIQ** must be tied off to HIGH because the internal GIC CPU interface generates the virtual interrupt signals to the cores. Software controls the **nIRQ** and **nFIQ** signals, therefore there is no requirement to tie them HIGH. If you disable the GIC CPU interface, a GIC that is external to the processor can drive the input signals **nVIRQ** and **nVFIQ**.

Asserting the **GICCDISABLE** signal HIGH at reset removes access to the memory-mapped and system GIC CPU Interface registers.

Related information

[B1.51 AArch64 Processor Feature Register 0, EL1](#) on page B1-217.

A12.2 Memory map for the GIC CPU interface

The GIC CPU Interface is a memory-mapped interface. It is offset from **PERIPHBASE**.

If **GICCDISABLE** is asserted, the registers are not available.

Table A12-1 GIC memory map

Address range	Functional block
0x00000-0x01FFF	CPU Interface
0x02000-0x0FFFF	Reserved
0x10000-0x10FFF	Virtual Interface Control
0x11000-0x1FFFF	Reserved
0x20000-0x21FFF	Virtual CPU Interface
0x22000-0x2EFFF	Reserved
0x2F000-0x30FFF	Alias of Virtual CPU Interface
0x31000-0x3FFFF	Reserved

Related information

B1.51 AArch64 Processor Feature Register 0, EL1 on page B1-217.

Part B
Register Descriptions

Chapter B1

AArch64 system registers

This chapter describes the system registers in the AArch64 state.

It contains the following sections:

- *B1.1 AArch64 register summary* on page B1-140.
- *B1.2 AArch64 Identification registers* on page B1-141.
- *B1.3 AArch64 Exception handling registers* on page B1-142.
- *B1.4 AArch64 Virtual memory control registers* on page B1-143.
- *B1.5 AArch64 Other System control registers* on page B1-145.
- *B1.6 AArch64 Cache maintenance operations* on page B1-146.
- *B1.7 AArch64 TLB maintenance operations* on page B1-147.
- *B1.8 AArch64 Address translation operations* on page B1-148.
- *B1.9 AArch64 Miscellaneous operations* on page B1-149.
- *B1.10 AArch64 Performance monitor registers* on page B1-150.
- *B1.11 AArch64 Reset registers* on page B1-152.
- *B1.12 AArch64 Secure registers* on page B1-153.
- *B1.13 AArch64 Virtualization registers* on page B1-154.
- *B1.14 AArch64 EL2 TLB maintenance operations* on page B1-155.
- *B1.15 AArch64 GIC system registers* on page B1-156.
- *B1.16 AArch64 Generic Timer registers* on page B1-158.
- *B1.17 AArch64 Thread registers* on page B1-159.
- *B1.18 AArch64 Implementation defined registers* on page B1-160.
- *B1.19 Auxiliary Control Register, EL1* on page B1-162.
- *B1.20 Auxiliary Control Register, EL2* on page B1-163.
- *B1.21 Auxiliary Control Register, EL3* on page B1-165.
- *B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3* on page B1-167.
- *B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3* on page B1-168.

- *B1.24 Auxiliary ID Register, EL1* on page B1-169.
- *B1.25 Auxiliary Memory Attribute Indirection Register, EL1* on page B1-170.
- *B1.26 Auxiliary Memory Attribute Indirection Register, EL2* on page B1-171.
- *B1.27 Auxiliary Memory Attribute Indirection Register, EL3* on page B1-172.
- *B1.28 Configuration Base Address Register, EL1* on page B1-173.
- *B1.29 Cache Size ID Register, EL1* on page B1-174.
- *B1.30 Cache Level ID Register, EL1* on page B1-176.
- *B1.31 Architectural Feature Access Control Register, EL1* on page B1-178.
- *B1.32 Architectural Feature Trap Register, EL2* on page B1-180.
- *B1.33 Architectural Feature Trap Register, EL3* on page B1-182.
- *B1.34 CPU Auxiliary Control Register, EL1* on page B1-184.
- *B1.35 CPU Extended Control Register, EL1* on page B1-187.
- *B1.36 CPU Memory Error Syndrome Register, EL1* on page B1-189.
- *B1.37 Cache Type Register, EL0* on page B1-192.
- *B1.38 Data Cache Zero ID Register, EL0* on page B1-194.
- *B1.39 Exception Syndrome Register, EL1* on page B1-195.
- *B1.40 Exception Syndrome Register, EL2* on page B1-197.
- *B1.41 Exception Syndrome Register, EL3* on page B1-199.
- *B1.42 Fault Address Register, EL1* on page B1-201.
- *B1.43 Fault Address Register, EL2* on page B1-202.
- *B1.44 Fault Address Register, EL3* on page B1-203.
- *B1.45 Hyp Auxiliary Configuration Register, EL2* on page B1-204.
- *B1.46 Hypervisor Configuration Register, EL2* on page B1-205.
- *B1.47 Hypervisor IPA Fault Address Register, EL2* on page B1-211.
- *B1.48 Hyp System Trap Register, EL2* on page B1-212.
- *B1.49 AArch64 Debug Feature Register 0, EL1* on page B1-213.
- *B1.50 AArch64 Instruction Set Attribute Register 0, EL1* on page B1-215.
- *B1.51 AArch64 Processor Feature Register 0, EL1* on page B1-217.
- *B1.52 AArch64 Memory Model Feature Register 0, EL1* on page B1-219.
- *B1.53 Interrupt Status Register, EL1* on page B1-221.
- *B1.54 L2 Auxiliary Control Register, EL1* on page B1-222.
- *B1.55 L2 Control Register, EL1* on page B1-224.
- *B1.56 L2 Extended Control Register, EL1* on page B1-226.
- *B1.57 L2 Memory Error Syndrome Register, EL1* on page B1-228.
- *B1.58 Memory Attribute Indirection Register, EL1* on page B1-231.
- *B1.59 Memory Attribute Indirection Register, EL2* on page B1-233.
- *B1.60 Memory Attribute Indirection Register, EL3* on page B1-234.
- *B1.61 Monitor Debug Configuration Register, EL2* on page B1-235.
- *B1.62 Monitor Debug Configuration Register, EL3* on page B1-238.
- *B1.63 Monitor Debug System Control Register, EL1* on page B1-240.
- *B1.64 Main ID Register, EL1* on page B1-243.
- *B1.65 Multiprocessor Affinity Register, EL1* on page B1-245.
- *B1.66 Physical Address Register, EL1* on page B1-247.
- *B1.67 Revision ID Register, EL1* on page B1-250.
- *B1.68 Reset Management Register, EL3* on page B1-251.
- *B1.69 Reset Vector Base Address Register, EL3* on page B1-252.
- *B1.70 Secure Configuration Register, EL3* on page B1-253.
- *B1.71 System Control Register, EL1* on page B1-256.
- *B1.72 System Control Register, EL2* on page B1-259.
- *B1.73 System Control Register, EL3* on page B1-261.
- *B1.74 Translation Control Register, EL1* on page B1-263.
- *B1.75 Translation Control Register, EL2* on page B1-267.
- *B1.76 Translation Control Register, EL3* on page B1-269.
- *B1.77 Translation Table Base Register 0, EL1* on page B1-271.
- *B1.78 Translation Table Base Register 0, EL3* on page B1-272.
- *B1.79 Translation Table Base Register 1, EL1* on page B1-273.

- *B1.80 Vector Base Address Register, EL1* on page B1-274.
- *B1.81 Vector Base Address Register, EL2* on page B1-275.
- *B1.82 Vector Base Address Register, EL3* on page B1-276.
- *B1.83 Virtualization Multiprocessor ID Register, EL2* on page B1-277.
- *B1.84 Virtualization Processor ID Register, EL2* on page B1-278.
- *B1.85 Virtualization Translation Control Register, EL2* on page B1-279.

B1.1 AArch64 register summary

This section gives a summary of the system registers in the AArch64 Execution state.

For more information on using the system registers, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

The following subsections describe the system registers by functional group:

- *B1.2 AArch64 Identification registers on page B1-141.*
- *B1.3 AArch64 Exception handling registers on page B1-142.*
- *B1.4 AArch64 Virtual memory control registers on page B1-143.*
- *B1.5 AArch64 Other System control registers on page B1-145.*
- *B1.6 AArch64 Cache maintenance operations on page B1-146.*
- *B1.7 AArch64 TLB maintenance operations on page B1-147.*
- *B1.8 AArch64 Address translation operations on page B1-148.*
- *B1.9 AArch64 Miscellaneous operations on page B1-149.*
- *B1.10 AArch64 Performance monitor registers on page B1-150.*
- *B1.11 AArch64 Reset registers on page B1-152.*
- *B1.12 AArch64 Secure registers on page B1-153.*
- *B1.13 AArch64 Virtualization registers on page B1-154.*
- *B1.14 AArch64 EL2 TLB maintenance operations on page B1-155.*
- *B1.15 AArch64 GIC system registers on page B1-156.*
- *B1.16 AArch64 Generic Timer registers on page B1-158.*
- *B1.17 AArch64 Thread registers on page B1-159.*
- *B1.18 AArch64 Implementation defined registers on page B1-160.*

B1.2 AArch64 Identification registers

The following table shows the identification registers in AArch64 state.

Bits[63:32] are reset to 0x00000000 for all 64-bit registers in the table.

Table B1-1 AArch64 identification registers

Name	Type	Reset	Width	Description
MIDR_EL1	RO	0x410FD021	32	<i>B1.64 Main ID Register, EL1 on page B1-243</i>
MPIDR_EL1	RO	-	64	<i>B1.65 Multiprocessor Affinity Register, EL1 on page B1-245</i> The reset value depends on the primary inputs, CLUSTERIDAFF1 and CLUSTERIDAFF2 , and the number of cores that the device implements.
REVIDR_EL1	RO	0x00000000	32	<i>B1.67 Revision ID Register, EL1 on page B1-250</i>
ID_AA64PFR0_EL1	RO	0x01001111	64	<i>B1.51 AArch64 Processor Feature Register 0, EL1 on page B1-217</i> Bits [27:24] are 0x1 if the GIC CPU interface is present and enabled, and 0x0 otherwise. Bits [23:16] are 0x00 if the Advanced SIMD and floating-point support is implemented, and 0xFF otherwise.
ID_AA64DFR0_EL1	RO	0x10305106	64	<i>B1.49 AArch64 Debug Feature Register 0, EL1 on page B1-213</i>
ID_AA64AFR0_EL1	RO	0x00000000	64	AArch64 Auxiliary Feature Register 0
ID_AA64AFR1_EL1	RO	0x00000000	64	AArch64 Auxiliary Feature Register 1
ID_AA64ISAR0_EL1	RO	0x00011120	64	<i>B1.50 AArch64 Instruction Set Attribute Register 0, EL1 on page B1-215</i> ID_AA64ISAR0_EL1 has the value 0x00010000 if the Cryptographic Extension is not implemented and enabled.
ID_AA64MMFR0_EL1	RO	0x00101122	64	<i>B1.52 AArch64 Memory Model Feature Register 0, EL1 on page B1-219</i>
CCSIDR_EL1	RO	-	32	<i>B1.29 Cache Size ID Register, EL1 on page B1-174</i> The reset value depends on the implementation. See the register description for details.
CLIDR_EL1	RO	0x0A400023	64	<i>B1.30 Cache Level ID Register, EL1 on page B1-176</i> The reset value is 0x09200003 if the L2 cache is not implemented. The reset value is 0x0A200023 if the L2 cache is implemented and BROADCASTINNER is set to 0. The reset value is 0x0A400023 if the L2 cache is implemented and BROADCASTINNER is set to 1.
AIDR_EL1	RO	0x00000000	32	<i>B1.24 Auxiliary ID Register, EL1 on page B1-169</i>
CSSELR_EL1	RW	0x00000000	32	<i>Cache Size Selection Register, EL1</i>
CTR_EL0	RO	0x84448004	32	<i>B1.37 Cache Type Register, EL0 on page B1-192</i>
DCZID_EL0	RO	0x00000004	32	<i>B1.38 Data Cache Zero ID Register, EL0 on page B1-194</i>
VPIDR_EL2	RW	0x410FD021	32	<i>B1.84 Virtualization Processor ID Register, EL2 on page B1-278</i>
VMPIDR_EL2	RO	-	64	<i>B1.83 Virtualization Multiprocessor ID Register, EL2 on page B1-277</i> The reset value is the value of the Multiprocessor Affinity Register.

B1.3 AArch64 Exception handling registers

The following table shows the fault handling registers in AArch64 state.

Bits[63:32] are reset to 0x00000000 for all 64-bit registers in the table.

Table B1-2 AArch64 exception handling registers

Name	Type	Reset	Width	Description
AFSR0_EL1	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3 on page B1-167</i>
AFSR1_EL1	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3 on page B1-168</i>
ESR_EL1	RW	UNK	32	<i>B1.39 Exception Syndrome Register, EL1 on page B1-195</i>
AFSR0_EL2	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3 on page B1-167</i>
AFSR1_EL2	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3 on page B1-168</i>
ESR_EL2	RW	UNK	32	<i>B1.40 Exception Syndrome Register, EL2 on page B1-197</i>
AFSR0_EL3	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3 on page B1-167</i>
AFSR1_EL3	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3 on page B1-168</i>
ESR_EL3	RW	UNK	32	<i>B1.41 Exception Syndrome Register, EL3 on page B1-199</i>
FAR_EL1	RW	UNK	64	<i>B1.42 Fault Address Register, EL1 on page B1-201</i>
FAR_EL2	RW	UNK	64	<i>B1.43 Fault Address Register, EL2 on page B1-202</i>
HPFAR_EL2	RW	0x0000000000000000	64	<i>B1.47 Hypervisor IPA Fault Address Register, EL2 on page B1-211</i>
FAR_EL3	RW	UNK	64	<i>B1.44 Fault Address Register, EL3 on page B1-203</i>
VBAR_EL1	RW	UNK	64	<i>B1.80 Vector Base Address Register, EL1 on page B1-274</i>
ISR_EL1	RO	UNK	32	<i>B1.53 Interrupt Status Register, EL1 on page B1-221</i>
VBAR_EL2	RW	UNK	64	<i>B1.81 Vector Base Address Register, EL2 on page B1-275</i>
VBAR_EL3	RW	UNK	64	<i>B1.82 Vector Base Address Register, EL3 on page B1-276</i>

B1.4 AArch64 Virtual memory control registers

The following table shows the virtual memory control registers in AArch64 state.

Bits[63:32] are reset to 0x00000000 for all 64-bit registers in the table.

Table B1-3 AArch64 virtual memory control registers

Name	Type	Reset	Width	Description
SCTLR_EL1	RW	0x30C50998	32	<i>B1.71 System Control Register, EL1</i> on page B1-256 The reset value depends on primary input CFGEND . The value listed here assumes this signal is LOW.
SCTLR_EL2	RW	0x30C50838	32	<i>B1.72 System Control Register, EL2</i> on page B1-259 The reset value depends on primary input CFGEND . The value listed here assumes this signal is LOW.
SCTLR_EL3	RW	0x30C50838	32	<i>B1.73 System Control Register, EL3</i> on page B1-261 The reset value depends on primary input CFGEND . The value listed here assumes this signal is LOW.
TTBR0_EL1	RW	UNK	64	<i>B1.77 Translation Table Base Register 0, EL1</i> on page B1-271
TTBR1_EL1	RW	UNK	64	<i>B1.79 Translation Table Base Register 1, EL1</i> on page B1-273
TCR_EL1	RW	UNK	64	<i>B1.74 Translation Control Register, EL1</i> on page B1-263
TTBR0_EL2	RW	UNK	64	Translation Table Base Address Register 0, EL2 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> .
TCR_EL2	RW	UNK	32	<i>B1.75 Translation Control Register, EL2</i> on page B1-267
VTTBR_EL2	RW	UNK	64	Virtualization Translation Table Base Address Register, EL2 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> .
VTCR_EL2	RW	UNK	32	<i>B1.85 Virtualization Translation Control Register, EL2</i> on page B1-279
TTBR0_EL3	RW	UNK	64	<i>B1.78 Translation Table Base Register 0, EL3</i> on page B1-272
TCR_EL3	RW	UNK	32	<i>B1.76 Translation Control Register, EL3</i> on page B1-269
MAIR_EL1	RW	UNK	64	<i>B1.58 Memory Attribute Indirection Register, EL1</i> on page B1-231
AMAIR_EL1	RW	0x0000000000000000	64	<i>B1.25 Auxiliary Memory Attribute Indirection Register, EL1</i> on page B1-170
MAIR_EL2	RW	UNK	64	<i>B1.59 Memory Attribute Indirection Register, EL2</i> on page B1-233
AMAIR_EL2	RW	0x0000000000000000	64	<i>B1.26 Auxiliary Memory Attribute Indirection Register, EL2</i> on page B1-171
MAIR_EL3	RW	UNK	64	<i>B1.60 Memory Attribute Indirection Register, EL3</i> on page B1-234

Table B1-3 AArch64 virtual memory control registers (continued)

Name	Type	Reset	Width	Description
AMAIR_EL3	RW	0x0000000000000000	64	<i>B1.27 Auxiliary Memory Attribute Indirection Register, EL3</i> on page B1-172
CONTEXTIDR_EL1	RW	UNK	32	Context ID Register, EL1 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> .

B1.5 AArch64 Other System control registers

The following table shows the other system control registers in AArch64 state.

Table B1-4 AArch64 other system control registers

Name	Type	Reset	Width	Description
ACTLR_EL1	RW	0x00000000	32	B1.19 Auxiliary Control Register, EL1 on page B1-162
CPACR_EL1	RW	0x00000000	32	B1.31 Architectural Feature Access Control Register, EL1 on page B1-178
ACTLR_EL2	RW	0x00000000	32	B1.20 Auxiliary Control Register, EL2 on page B1-163
ACTLR_EL3	RW	0x00000000	32	B1.21 Auxiliary Control Register, EL3 on page B1-165

B1.6 AArch64 Cache maintenance operations

The following table shows the System instructions for cache and maintenance operations in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information about these operations.

Table B1-5 AArch64 cache maintenance operations

Name	Description
IC IALLUIS	Instruction cache invalidate all to PoU Inner Shareable PoU = Point of Unification. PoU is set by the BROADCASTINNER signal and can be in the L1 data cache or outside of the processor, in which case PoU is dependent on the external memory system.
IC IALLU	Instruction cache invalidate all to PoU
IC IVAU	Instruction cache invalidate by <i>virtual address (VA)</i> to PoU
DC IVAC	Data cache invalidate by VA to PoC PoC = Point of Coherence. The PoC is always outside of the processor and depends on the external memory system.
DC ISW	Data cache invalidate by set/way
DC CSW	Data cache clean by set/way
DC CISW	Data cache clean and invalidate by set/way
DC ZVA	Data cache zero by VA
DC CVAC	Data cache clean by VA to PoC
DC CVAU	Data cache clean by VA to PoU
DC CIVAC	Data cache clean and invalidate by VA to PoC

B1.7 AArch64 TLB maintenance operations

The following table shows the System instructions for TLB maintenance operations in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information about these operations.

Table B1-6 AArch64 TLB maintenance operations

Name	Description
TLBI VMALLE1IS	Invalidate all stage 1 translations used at EL1 with the current <i>virtual machine identifier</i> (VMID) in the Inner Shareable
TLBI VAE1IS	Invalidate translation used at EL1 for the specified VA and <i>Address Space Identifier</i> (ASID) and the current VMID, Inner Shareable
TLBI ASIDE1IS	Invalidate all translations used at EL1 with the current VMID and the supplied ASID, Inner Shareable
TLBI VAAE1IS	Invalidate all translations used at EL1 for the specified address and current VMID and for all ASID values, Inner Shareable
TLBI VALE1IS	Invalidate all entries from the last level of stage 1 translation table walk used at EL1 with the supplied ASID and current VMID, Inner Shareable
TLBI VAALE1IS	Invalidate all entries from the last level of stage 1 translation table walk used at EL1 for the specified address and current VMID and for all ASID values, Inner Shareable
TLBI VMALLE1	Invalidate all stage 1 translations used at EL1 with the current VMID
TLBI VAE1	Invalidate translation used at EL1 for the specified VA and ASID and the current VMID
TLBI ASIDE1	Invalidate all translations used at EL1 with the current VMID and the supplied ASID
TLBI VAAE1	Invalidate all translations used at EL1 for the specified address and current VMID and for all ASID values
TLBI VALE1	Invalidate all entries from the last level of stage 1 translation table walk used at EL1 with the supplied ASID and current VMID
TLBI VAALE1	Invalidate all entries from the last level of stage 1 translation table walk used at EL1 for the specified address and current VMID and for all ASID values

The Virtualization registers include additional TLB operations for use in Hyp mode. For more information, see [B1.14 AArch64 EL2 TLB maintenance operations](#) on page B1-155.

B1.8 AArch64 Address translation operations

The following table shows the address translation register in AArch64 state.

Table B1-7 AArch64 address translation register

Name	Type	Reset	Width	Description
PAR_EL1	RW	UNK	64	<i>B1.66 Physical Address Register, EL1 on page B1-247</i>

The following table shows the System instructions for address translation operations in AArch64 state. See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

Table B1-8 AArch64 address translation operations

Name	Description
AT S1E1R	Stage 1 current state EL1 read
AT S1E1W	Stage 1 current state EL1 write
AT S1E0R	Stage 1 current state unprivileged read
AT S1E0W	Stage 1 current state unprivileged write
AT S1E2R	Stage 1 Hyp mode read
AT S1E2W	Stage 1 Hyp mode write
AT S12E1R	Stages 1 and 2 Non-secure EL1 read
AT S12E1W	Stages 1 and 2 Non-secure EL1 write
AT S12E0R	Stages 1 and 2 Non-secure unprivileged read
AT S12E0W	Stages 1 and 2 Non-secure unprivileged write
AT S1E3R	Stage 1 current state EL3 read
AT S1E3W	Stage 1 current state EL3 write

B1.9 AArch64 Miscellaneous operations

The following table shows the miscellaneous operations in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information about these operations.

Table B1-9 AArch64 miscellaneous system operations

Name	Type	Reset	Width	Description
TPIDR_EL0	RW	UNK	64	Thread Pointer / ID Register, EL0
TPIDR_EL1	RW	UNK	64	Thread Pointer / ID Register, EL1
TPIDRRO_EL0	RW RO at EL0.	UNK	64	Thread Pointer / ID Register, read-only, EL0
TPIDR_EL2	RW	UNK	64	Thread Pointer / ID Register, EL2
TPIDR_EL3	RW	UNK	64	Thread Pointer / ID Register, EL3

B1.10 AArch64 Performance monitor registers

The following table shows the performance monitor registers in AArch64 state.

Bits[63:32] are reset to 0x00000000 for all 64-bit registers in the table.

Table B1-10 AArch64 performance monitor registers

Name	Type	Reset	Width	Description
PMCR_EL0	RW	0x41083040	32	C9.2 Performance Monitors Control Register, EL0 on page C9-397
PMCNTENSET_EL0	RW	UNK	32	Performance Monitors Count Enable Set Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMCNTENCLR_EL0	RW	UNK	32	Performance Monitors Count Enable Clear Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMOVSLR_EL0	RW	UNK	32	Performance Monitors Overflow Flag Status Clear Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMSWINC_EL0	WO	-	32	Performance Monitors Software Increment Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMSELR_EL0	RW	UNK	32	Performance Monitors Event Counter Selection Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMCEID0_EL0	RO	0x6FFFBF00	32	C9.3 Performance Monitors Common Event Identification Register 0, EL0 on page C9-399 The reset value is 0x6E3FBFFF if the Cortex-A34 processor has not been configured with an L2 cache.
PMCEID1_EL0	RO	0x00000000	32	C9.4 Performance Monitors Common Event Identification Register 1, EL0 on page C9-403 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMCCNTR_EL0	RW	UNK	64	Performance Monitors Cycle Counter See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMXEVTYPER_EL0	RW	UNK	32	Performance Monitors Selected Event Type and Filter Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMXVCNTR_EL0	RW	UNK	32	Performance Monitors Selected Event Counter Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.

Table B1-10 AArch64 performance monitor registers (continued)

Name	Type	Reset	Width	Description
PMUSERENR_EL0	RW	0x00000000	32	Performance Monitors User Enable Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMINTENSET_EL1	RW	UNK	32	Performance Monitors Interrupt Enable Set Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMINTENCLR_EL1	RW	UNK	32	Performance Monitors Interrupt Enable Clear Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMOVSSET_EL0	RW	UNK	32	Performance Monitors Overflow Flag Status Set Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
PMEVCNTR0_EL0	RW	UNK	32	Performance Monitor Event Count Registers
PMEVCNTR1_EL0	RW	UNK	32	
PMEVCNTR2_EL0	RW	UNK	32	
PMEVCNTR3_EL0	RW	UNK	32	
PMEVCNTR4_EL0	RW	UNK	32	
PMEVCNTR5_EL0	RW	UNK	32	
PMEVTYPER0_EL0	RW	UNK	32	Performance Monitor Event Type Registers
PMEVTYPER1_EL0	RW	UNK	32	
PMEVTYPER2_EL0	RW	UNK	32	
PMEVTYPER3_EL0	RW	UNK	32	
PMEVTYPER4_EL0	RW	UNK	32	
PMEVTYPER5_EL0	RW	UNK	32	
PMCCFILTR_EL0	RW	0x00000000	32	Performance Monitors Cycle Count Filter Register See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.

B1.11 AArch64 Reset registers

The following table shows the reset registers in AArch64 state.

Table B1-11 AArch64 reset management registers

Name	Type	Reset	Width	Description
RVBAR_EL3	RO	-	64	<i>B1.69 Reset Vector Base Address Register, EL3</i> on page B1-252 The reset value depends on the RVBARADDR signal.
RMR_EL3	RW	0x00000001	32	<i>B1.68 Reset Management Register, EL3</i> on page B1-251

B1.12 AArch64 Secure registers

The following table shows the secure registers in AArch64 state.

Table B1-12 AArch64 security registers

Name	Type	Reset	Width	Description
SCR_EL3	RW	0x00000430	32	<i>B1.70 Secure Configuration Register, EL3 on page B1-253</i>
CPTR_EL3	RW	0x00000000	32	<i>B1.33 Architectural Feature Trap Register, EL3 on page B1-182</i> Reset value is 0x00000000 if Advanced SIMD and floating-point are implemented, 0x00000400 otherwise.
MDCR_EL3	RW	0x00000000	32	<i>B1.62 Monitor Debug Configuration Register, EL3 on page B1-238</i>
AFSR0_EL3	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3 on page B1-167</i>
AFSR1_EL3	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3 on page B1-168</i>
VBAR_EL3	RW	UNK	64	<i>B1.82 Vector Base Address Register, EL3 on page B1-276</i>

B1.13 AArch64 Virtualization registers

The following table shows the virtualization registers in AArch64 state.

Bits[63:32] are reset to 0x00000000 for all 64-bit registers in this table.

Table B1-13 AArch64 virtualization registers

Name	Type	Reset	Width	Description
VPIDR_EL2	RW	0x410FD021	32	<i>B1.84 Virtualization Processor ID Register, EL2</i> on page B1-278
VMPIDR_EL2	RW	-	64	<i>B1.83 Virtualization Multiprocessor ID Register, EL2</i> on page B1-277 The reset value is the value of the Multiprocessor Affinity Register.
SCTLR_EL2	RW	0x30C50838	32	<i>B1.72 System Control Register, EL2</i> on page B1-259 The reset value depends on CFGEND . The value shown assumes this signal is set to LOW.
ACTLR_EL2	RW	0x00000000	32	<i>B1.20 Auxiliary Control Register, EL2</i> on page B1-163
HCR_EL2	RW	0x0000000080000002	64	<i>B1.46 Hypervisor Configuration Register, EL2</i> on page B1-205
MDCR_EL2	RW	0x00000006	32	<i>B1.61 Monitor Debug Configuration Register, EL2</i> on page B1-235
CPTR_EL2	RW	0x000033FF	32	<i>B1.32 Architectural Feature Trap Register, EL2</i> on page B1-180 The reset value is 0x000037FF if Advances SIMD and floating-point are not implemented.
HSTR_EL2	RW	0x00000000	32	<i>B1.48 Hyp System Trap Register, EL2</i> on page B1-212
HACR_EL2	RW	0x00000000	32	<i>B1.45 Hyp Auxiliary Configuration Register, EL2</i> on page B1-204
TTBR0_EL2	RW	UNK	64	Translation Table Base Address Register 0, EL3 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> for more information.
TCR_EL2	RW	UNK	32	<i>B1.75 Translation Control Register, EL2</i> on page B1-267
VTTBR_EL2	RW	UNK	64	Virtualization Translation Table Base Address Register, EL2 See the <i>ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile</i> .
VTCR_EL2	RW	UNK	32	<i>B1.85 Virtualization Translation Control Register, EL2</i> on page B1-279
AFSR0_EL2	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3</i> on page B1-167
AFSR1_EL2	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3</i> on page B1-168
ESR_EL2	RW	UNK	32	<i>B1.40 Exception Syndrome Register, EL2</i> on page B1-197
FAR_EL2	RW	UNK	64	<i>B1.43 Fault Address Register, EL2</i> on page B1-202
HPFAR_EL2	RW	UNK	64	<i>B1.47 Hypervisor IPA Fault Address Register, EL2</i> on page B1-211
MAIR_EL2	RW	UNK	64	<i>B1.59 Memory Attribute Indirection Register, EL2</i> on page B1-233
AMAIR_EL2	RW	0x0000000000000000	64	<i>B1.26 Auxiliary Memory Attribute Indirection Register, EL2</i> on page B1-171
VBAR_EL2	RW	UNK	64	<i>B1.81 Vector Base Address Register, EL2</i> on page B1-275

B1.14 AArch64 EL2 TLB maintenance operations

The following table shows the System instructions for TLB maintenance operations added in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information about these operations.

Table B1-14 AArch64 TLB maintenance operations

Name	Description
TLBI IPAS2E1IS	Invalidate stage 2 only translations used at EL1 for the specified IPA for the current VMID, Inner Shareable
TLBI IPAS2LE1IS	Invalidate entries from the last level of stage 2 only translation used at EL1 for the specified IPA for the current VMID, Inner Shareable
TLBI ALLE2IS	Invalidate all stage 1 translations used at EL2, Inner Shareable
TLBI VAE2IS	Invalidate translation used at EL2 for the specified VA and ASID and the current VMID, Inner Shareable
TLBI ALLE1IS	Invalidate all stage 1 translations used at EL1, Inner Shareable
TLBI VALE2IS	Invalidate all entries from the last level of stage 1 translation table walk used at EL2 with the supplied ASID and current VMID, Inner Shareable
TLBI VMALLS12E1IS	Invalidate all stage 1 and 2 translations used at EL1 with the current VMID, Inner Shareable
TLBI IPAS2E1	Invalidate stage 2 only translations used at EL1 for the specified IPA for the current VMID
TLBI IPAS2LE1	Invalidate entries from the last level of stage 2 only translation used at EL1 for the specified IPA for the current VMID
TLBI ALLE2	Invalidate all stage 1 translations used at EL2
TLBI VAE2	Invalidate translation used at EL2 for the specified VA and ASID and the current VMID
TLBI ALLE1	Invalidate all stage 1 translations used at EL1
TLBI VALE2	Invalidate all entries from the last level of stage 1 translation table walk used at EL2 with the supplied ASID and current VMID
TLBI VMALLS12E1	Invalidate all stage 1 and 2 translations used at EL1 with the current VMID
TLBI ALLE3IS	Invalidate all stage 1 translations used at EL3, Inner Shareable
TLBI VAE3IS	Invalidate translation used at EL3 for the specified VA and ASID and the current VMID, Inner Shareable
TLBI VALE3IS	Invalidate all entries from the last level of stage 1 translation table walk used at EL3 with the supplied ASID and current VMID, Inner Shareable
TLBI ALLE3	Invalidate all stage 1 translations used at EL3
TLBI VAE3	Invalidate translation used at EL3 for the specified VA and ASID and the current VMID
TLBI VALE3	Invalidate all entries from the last level of stage 1 translation table walk used at EL3 with the supplied ASID and current VMID

B1.15 AArch64 GIC system registers

The following table shows the GIC system registers in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

Table B1-15 GIC system registers

Name	Type	Reset	Width	Description
ICC_AP0R0_EL1	RW	0x00000000	32	Active Priorities 0 Register 0
ICC_AP1R0_EL1	RW	0x00000000	32	Active Priorities 1 Register 0
ICC_ASGI1R_EL1	WO	-	64	Alternate SGI Generation Register 1
ICC_BPR0_EL1	RW	0x00000002	32	Binary Point Register 0
ICC_BPR1_EL1	RW	0x00000003	32	Binary Point Register 1 This is the reset value in Non-secure states. In Secure states, the reset value is 0x00000002.
ICC_CTLR_EL1	RW	0x00000400	32	Interrupt Control Register for EL1
ICC_CTLR_EL3	RW	0x00000400	32	Interrupt Control Register for EL3
ICC_DIR_EL1	WO	-	32	Deactivate Interrupt Register
ICC_EOIR0_EL1	WO	-	32	End Of Interrupt Register 0
ICC_EOIR1_EL1	WO	-	32	End Of Interrupt Register 1
ICC_HPPIR0_EL1	RO	-	32	Highest Priority Pending Interrupt Register 0
ICC_HPPIR1_EL1	RO	-	32	Highest Priority Pending Interrupt Register 1
ICC_IAR0_EL1	RO	-	32	Interrupt Acknowledge Register 0
ICC_IAR1_EL1	RO	-	32	Interrupt Acknowledge Register 1
ICC_IGRPEN0_EL1	RW	0x00000000	32	Interrupt Group Enable Register 0
ICC_IGRPEN1_EL1	RW	0x00000000	32	Interrupt Group Enable Register 1
ICC_IGRPEN1_EL3	RW	0x00000000	32	Interrupt Group Enable Register 1 for EL3
ICC_PMR_EL1	RW	0x00000000	32	Priority Mask Register
ICC_RPR_EL1	RO	-	32	Running Priority Register
ICC_SGI0R_EL1	WO	-	64	SGI Generation Register 0
ICC_SGI1R_EL1	WO	-	64	SGI Generation Register 1
ICC_SRE_EL1	RW	0x00000000	32	System Register Enable Register for EL1
ICC_SRE_EL2	RW	0x00000000	32	System Register Enable Register for EL2
ICC_SRE_EL3	RW	0x00000000	32	System Register Enable Register for EL3
ICH_AP0R0_EL2	RW	0x00000000	32	Interrupt Controller Hyp Active Priorities Register (0,0)
ICH_AP1R0_EL2	RW	0x00000000	32	Interrupt Controller Hyp Active Priorities Register (1,0)
ICH_EISR_EL2	RO	0x00000000	32	Interrupt Controller End of Interrupt Status Register
ICH_ELRSR_EL2	RO	0x0000000F	32	Interrupt Controller Empty List Register Status Register

Table B1-15 GIC system registers (continued)

Name	Type	Reset	Width	Description
ICH_HCR_EL2	RW	0x00000000	32	Interrupt Controller Hyp Control Register
ICH_LR0_EL2	RW	0x0000000000000000	64	Interrupt Controller List Register 0
ICH_LR1_EL2	RW	0x0000000000000000	64	Interrupt Controller List Register 1
ICH_LR2_EL2	RW	0x0000000000000000	64	Interrupt Controller List Register 2
ICH_LR3_EL2	RW	0x0000000000000000	64	Interrupt Controller List Register 3
ICH_MISR_EL2	RO	0x00000000	32	Interrupt Controller Maintenance Interrupt State Register
ICH_VMCR_EL2	RW	0x004C0000	32	Interrupt Controller Virtual Machine Control Register
ICH_VTR_EL2	RO	0x90080003	32	Interrupt Controller VGIC Type Register

B1.16 AArch64 Generic Timer registers

The processor implements the architecturally defined Generic Timer registers.

Related information

- [B3.1 AArch64 Generic Timer register summary on page B3-292.](#)
- *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* (ARM DDI 0487).

B1.17 AArch64 Thread registers

The following table shows the thread registers in AArch64 state.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information about these operations.

Table B1-16 AArch64 miscellaneous system control operations

Name	Type	Reset	Width	Description
TPIDR_EL0	RW	UNK	64	Thread Pointer/ID Register, EL0
TPIDR_EL1	RW	UNK	64	Thread Pointer/ID Register, EL1
TPIDRRO_EL0	RW	UNK	64	Thread Pointer/ID Register, read-only, EL0
TPIDR_EL2	RW	UNK	64	Thread Pointer/ID Register, EL2
TPIDR_EL3	RW	UNK	64	Thread Pointer/ID Register, EL3

B1.18 AArch64 Implementation defined registers

IMPLEMENTATION DEFINED registers provide test features and any required configuration options specific to the Cortex-A34 processor.

The following table shows the IMPLEMENTATION DEFINED registers in AArch64 state.

Table B1-17 AArch64 implementation defined registers

Name	Type	Reset	Width	Description
ACTLR_EL1	RW	0x00000000	32	<i>B1.19 Auxiliary Control Register, EL1</i> on page B1-162
ACTLR_EL2	RW	0x00000000	32	<i>B1.20 Auxiliary Control Register, EL2</i> on page B1-163
ACTLR_EL3	RW	0x00000000	32	<i>B1.21 Auxiliary Control Register, EL3</i> on page B1-165
AFSR0_EL1	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3</i> on page B1-167
AFSR1_EL1	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3</i> on page B1-168
AFSR0_EL2	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3</i> on page B1-167
AFSR1_EL2	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3</i> on page B1-168
AFSR0_EL3	RW	0x00000000	32	<i>B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3</i> on page B1-167
AFSR1_EL3	RW	0x00000000	32	<i>B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3</i> on page B1-168
AMAIR_EL1	RW	0x0000000000000000	64	<i>B1.25 Auxiliary Memory Attribute Indirection Register, EL1</i> on page B1-170
AMAIR_EL2	RW	0x0000000000000000	64	<i>B1.26 Auxiliary Memory Attribute Indirection Register, EL2</i> on page B1-171
AMAIR_EL3	RW	0x0000000000000000	64	<i>B1.27 Auxiliary Memory Attribute Indirection Register, EL3</i> on page B1-172
L2CTLR_EL1	RW	-	32	<i>B1.55 L2 Control Register, EL1</i> on page B1-224 The reset value depends on the processor implementation and the state of the L2RSTDISABLE signal.
L2ECTLR_EL1	RW	0x00000000	32	<i>B1.56 L2 Extended Control Register, EL1</i> on page B1-226
L2ACTLR_EL1	RW	0x80000000	32	<i>B1.54 L2 Auxiliary Control Register, EL1</i> on page B1-222 This is the reset value for an ACE interface. For an AXI interface the reset value is 0x80000008. For a CHI interface the reset value is 0x80004008.
CPUACTLR_EL1	RW	0x00000000090CA000	64	<i>B1.34 CPU Auxiliary Control Register, EL1</i> on page B1-184
CPUECTLR_EL1	RW	0x0000000000000000	64	<i>B1.35 CPU Extended Control Register, EL1</i> on page B1-187
CPUMERRSR_EL1	RW	-	64	<i>B1.36 CPU Memory Error Syndrome Register, EL1</i> on page B1-189
L2MERRSR_EL1	RW	-	64	<i>B1.57 L2 Memory Error Syndrome Register, EL1</i> on page B1-228

Table B1-17 AArch64 implementation defined registers (continued)

Name	Type	Reset	Width	Description
CBAR_EL1	RO	-	64	<i>B1.28 Configuration Base Address Register, EL1</i> on page B1-173 The reset value depends on the PERIPHBASE signal.
CDBGDR0_EL3	RO	UNK	32	Cache Debug Data Register 0, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGDR1_EL3	RO	UNK	32	Cache Debug Data Register 1, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGDR2_EL3	RO	UNK	32	Cache Debug Data Register 2, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGDR3_EL3	RO	UNK	32	Cache Debug Data Register 3, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGDCT_EL3	WO	UNK	32	Cache Debug Data Cache Tag Read Operation Register, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGICT_EL3	WO	UNK	32	Cache Debug Instruction Cache Tag Read Operation Register, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGDCD_EL3	WO	UNK	32	Cache Debug Cache Debug Data Cache Data Read Operation Register, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGICD_EL3	WO	UNK	32	Cache Debug Instruction Cache Data Read Operation Register, see <i>C5.1 About direct access to internal memory</i> on page C5-328.
CDBGTD_EL3	WO	UNK	32	Cache Debug TLB Data Read Operation Register, see <i>C5.1 About direct access to internal memory</i> on page C5-328.

B1.19 Auxiliary Control Register, EL1

ACTLR_EL1

The processor does not implement the ACTLR_EL1 register. This register is always RES0.

B1.20 Auxiliary Control Register, EL2

The ACTLR_EL2 characteristics are:

Purpose

Controls write access to IMPLEMENTATION DEFINED registers in Non-secure EL1 modes, such as CPUACTLR, CPUECTLR, L2CTLR, L2ECTLR, and L2ACTLR.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

ACTLR_EL2 is a 32-bit register.

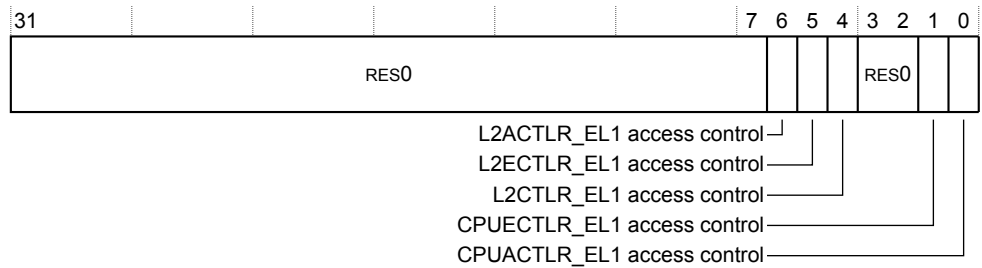


Figure B1-1 ACTLR_EL2 bit assignments

[31:7]

Reserved, RES0.

L2ACTLR_EL1 access control, [6]

L2ACTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from Non-secure EL1. This is the reset value.
- 1 The register is write accessible from Non-secure EL1.

Write access from Non-secure EL1 also requires ACTLR_EL3[6] to be set.

L2ECTLR_EL1 access control, [5]

L2ECTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from Non-secure EL1. This is the reset value.
- 1 The register is write accessible from Non-secure EL1.

Write access from Non-secure EL1 also requires ACTLR_EL3[5] to be set.

L2CTLR_EL1 access control, [4]

L2CTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from Non-secure EL1. This is the reset value.
- 1 The register is write accessible from Non-secure EL1.

Write access from Non-secure EL1 also requires ACTLR_EL3[4] to be set.

[3:2]

Reserved, RES0.

CPUECTLR_EL1 access control, [1]

CPUECTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from Non-secure EL1. This is the reset value.
- 1 The register is write accessible from Non-secure EL1.

Write access from Non-secure EL1 also requires ACTLR_EL3[1] to be set.

CPUACTLR_EL1 access control, [0]

CPUACTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from Non-secure EL1. This is the reset value.
- 1 The register is write accessible from Non-secure EL1.

Write access from Non-secure EL1 also requires ACTLR_EL3[0] to be set.

To access the ACTLR_EL2:

```
MRS <Xt>, ACTLR_EL2 ; Read ACTLR_EL2 into Xt
MSR ACTLR_EL2, <Xt> ; Write Xt to ACTLR_EL2
```

Register access is encoded as follows:

Table B1-18 ACTLR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0001	0000	001

B1.21 Auxiliary Control Register, EL3

The ACTLR_EL3 characteristics are:

Purpose

Controls write access to IMPLEMENTATION DEFINED registers in EL2, such as CPUACTLR, CPUECTLR, L2CTLR, L2ECTLR, and L2ACTLR.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

ACTLR_EL3 is a 32-bit register.

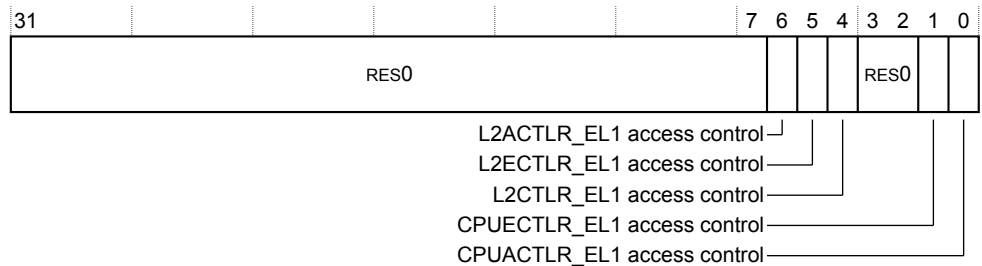


Figure B1-2 ACTLR_EL3 bit assignments

[31:7]

Reserved, RES0.

L2ACTLR_EL1 access control, [6]

L2ACTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from a lower exception level. This is the reset value.
- 1 The register is write accessible from EL2.

L2ECTLR_EL1 access control, [5]

L2ECTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from a lower exception level. This is the reset value.
- 1 The register is write accessible from EL2.

L2CTLR_EL1 access control, [4]

L2CTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from a lower exception level. This is the reset value.
- 1 The register is write accessible from EL2.

[3:2]

Reserved, RES0.

CPUECTLR_EL1 access control, [1]

CPUECTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from a lower exception level. This is the reset value.
- 1 The register is write accessible from EL2.

CPUACTLR_EL1 access control, [0]

CPUACTLR_EL1 write access control. The possible values are:

- 0 The register is not write accessible from a lower exception level. This is the reset value.
- 1 The register is write accessible from EL2.

To access the ACTLR_EL3:

```
MRS <Xt>, ACTLR_EL3 ; Read ACTLR_EL3 into Xt  
MSR ACTLR_EL3, <Xt> ; Write Xt to ACTLR_EL3
```

Register access is encoded as follows:

Table B1-19 ACTLR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0001	0000	001

B1.22 Auxiliary Fault Status Register 0, EL1, EL2, and EL3

AFSR0_EL1, AFSR0_EL2, and AFSR0_EL3

The processor does not implement AFSR0_EL1, AFSR0_EL2, and AFSR0_EL3. These registers are always RES0.

B1.23 Auxiliary Fault Status Register 1, EL1, EL2, and EL3

AFSR1_EL1, AFSR1_EL2, and AFSR1_EL3

The processor does not implement AFSR1_EL1, AFSR1_EL2, and AFSR1_EL3. These registers are always RES0.

B1.24 Auxiliary ID Register, EL1

AIDR_EL1

The processor does not implement AIDR_EL1. This register is always RES0.

B1.25 Auxiliary Memory Attribute Indirection Register, EL1

AMAIR_EL1

The processor does not implement AMAIR_EL1. This register is always RES0.

B1.26 Auxiliary Memory Attribute Indirection Register, EL2

AMAIR_EL2

The processor does not implement AMAIR_EL2. This register is always RES0.

B1.27 Auxiliary Memory Attribute Indirection Register, EL3

AMAIR_EL3

The processor does not implement AMAIR_EL3. This register is always RES0.

B1.28 Configuration Base Address Register, EL1

The CBAR_EL1 characteristics are:

Purpose

Holds the physical base address of the memory-mapped GIC CPU interface registers.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

Attributes

CBAR_EL1 is a 64-bit register.

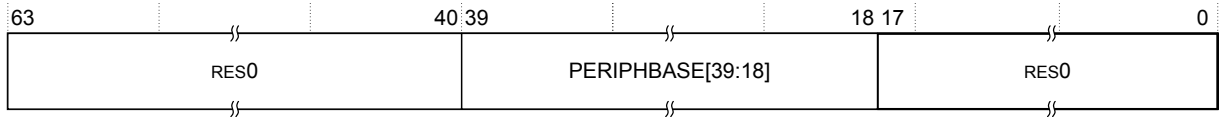


Figure B1-3 CBAR_EL1 bit assignments

[63:40]

Reserved, RES0.

PERIPHBASE[39:18], [39:18]

If the processor is implemented with the GIC CPU interface, the input **PERIPHBASE[39:18]** determines the reset value. If the GIC CPU interface is not implemented, this field is RAZ.

[17:0]

Reserved, RES0.

To access the CBAR_EL1:

```
MRS <Xt>, S3_1_C15_C3_0 ; Read CBAR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-20 CBAR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0011	000

B1.29 Cache Size ID Register, EL1

The CCSIDR_EL1 characteristics are:

Purpose

Provides information about the architecture of the caches.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

CCSIDR_EL1 is a 32-bit register.

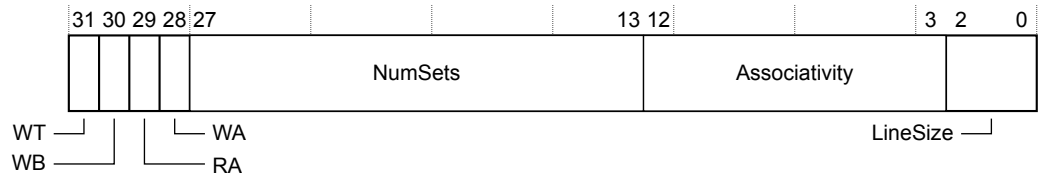


Figure B1-4 CCSIDR_EL1 bit assignments

WT, [31]

Indicates support for write-through:

0 Cache level does not support write-through.

WB, [30]

Indicates support for write-back:

0 Cache level does not support write-back.

1 Cache level supports write-back.

RA, [29]

Indicates support for Read-Allocation:

0 Cache level does not support Read-Allocation.

1 Cache level supports Read-Allocation.

WA, [28]

Indicates support for Write-Allocation:

0 Cache level does not support Write-Allocation.

1 Cache level supports Write-Allocation.

NumSets, [27:13]

Indicates the number of sets in cache - 1. Therefore, a value of 0 indicates 1 set in the cache. The number of sets does not have to be a power of 2.

For more information about encoding, see [Table B1-21 CCSIDR_EL1 encodings on page B1-175](#).

Associativity, [12:3]

Indicates the associativity of cache - 1. Therefore, a value of 0 indicates an associativity of 1. The associativity does not have to be a power of 2.

For more information about encoding, see [Table B1-21 CCSIDR_EL1 encodings](#) on page B1-175.

LineSize, [2:0]

Indicates the $(\log_2(\text{number of words in cache line})) - 2$:

0b010 16 words per line.

The following table shows the individual bit field and complete register encodings for the CCSIDR_EL1.

Table B1-21 CCSIDR_EL1 encodings

CSSELR	Cache	Size	Complete register encoding	Register bit field encoding						
				WT	WB	RA	WA	NumSets	Associativity	LineSize
0x0	L1 Data cache	8KB	0x7003E01A	0	1	1	1	0x001F	0x003	0x2
		16KB	0x7007E01A					0x003F	0x003	0x2
		32KB	0x700FE01A					0x007F	0x003	0x2
		64KB	0x701FE01A					0x00FF	0x003	0x2
0x1	L1 Instruction cache	8KB	0x2007E00A	0	0	1	0	0x003F	0x001	0x2
		16KB	0x200FE00A					0x007F	0x001	0x2
		32KB	0x201FE00A					0x00FF	0x001	0x2
		64KB	0x203FE00A					0x001F	0x001	0x2
0x2	L2 cache	128KB	0x700FE03A	0	1	1	1	0x00FF	0x007	0x2
		256KB	0x701FE03A					0x01FF	0x007	0x2
		512KB	0x703FE03A					0x03FF	0x007	0x2
		1024KB	0x707FE03A					0x07FF	0x007	0x2
0x3-0xF	Reserved	-	-	-	-	-	-	-	-	-

To access the CCSIDR_EL1:

```
MRS <Xt>, CCSIDR_EL1 ; Read CCSIDR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-22 CCSIDR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	0000	0000	000

B1.30 Cache Level ID Register, EL1

The CLIDR_EL1 characteristics are:

Purpose

Identifies:

- The type of cache, or caches, implemented at each level.
- The Level of Coherency and Level of Unification for the cache hierarchy.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

CLIDR_EL1 is a 64-bit register.

32	30	29	27	26	24	23	21	20				9	8	6	5	3	2	0
ICB		LoUU		LoC		LoUIS				RES0				Ctype3		Ctype2		Ctype1

Figure B1-5 CLIDR_EL1 bit assignments

[63:33]

Reserved, RES0.

ICB, [32:30]

Inner cache boundary. This field indicates the boundary between the inner and the outer domain.

0b000 Not disclosed in this mechanism.

LoUU, [29:27]

Indicates the Level of Unification Uniprocessor for the cache hierarchy:

0b001 L1 cache is the last level of cache that must be cleaned or invalidated when cleaning or invalidating to the point of unification for the processor.

LoC, [26:24]

Indicates the Level of Coherency for the cache hierarchy:

0b001 L2 cache not implemented. A clean to the point of coherency operation requires the L1 cache to be cleaned.

0b010 L2 cache implemented. A clean to the point of coherency operation requires the L1 and L2 caches to be cleaned.

LoUIS, [23:21]

Indicates the Level of Unification Inner Shareable for the cache hierarchy:

0b010 L2 cache.

L2 cache is the last level of cache that must be cleaned or invalidated when cleaning or invalidating to the point of unification for the Inner Shareable shareability domain.

If the processor is implemented without an L2 cache, or if **BROADCASTINNER** is set to 0, then LoUIS is 0b001, indicating the L1 cache.

[20:9]

Reserved, RES0.

Ctype3, [8:6]

Indicates the type of cache if the processor implements L3 cache:

0b000 L3 cache not implemented.

If software reads the Cache Type fields from Ctype1 upwards, after it has seen a value of 0b000, no caches exist at further-out levels of the hierarchy. So, for example, if Ctype2 is the first Cache Type field with a value of 0b000, the value of Ctype3 must be ignored.

Ctype2, [5:3]

Indicates the type of cache if the processor implements L2 cache:

0b000 L2 cache not implemented.

0b100 Unified instruction and data caches at L2.

Ctype1, [2:0]

Indicates the type of cache implemented at L1:

0b011 Separate instruction and data caches at L1.

To access the CLIDR_EL1:

```
MRS <Xt>, CLIDR_EL1 ; Read CLIDR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-23 CLIDR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	0000	0000	001

B1.31 Architectural Feature Access Control Register, EL1

The CPACR_EL1 characteristics are:

Purpose

Controls access to trace functionality and access to registers associated with Advanced SIMD and floating-point execution.

CPACR_EL1 is part of the Other system registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

CPACR_EL1 is a 32-bit register.

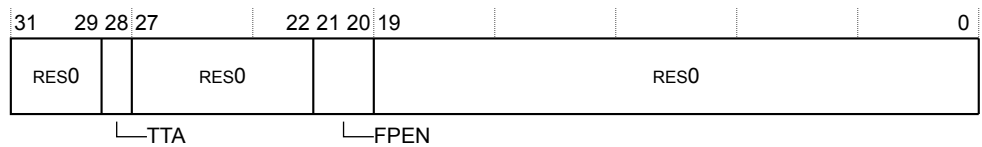


Figure B1-6 CPACR_EL1 bit assignments

[31:29]

Reserved, RES0.

TTA, [28]

Causes access to the Trace functionality to trap to EL1 when executed from EL0 or EL1.

This bit is RES0.

[27:22]

Reserved, RES0.

FPEN, [21:20]

Traps instructions that access registers associated with Advanced SIMD and floating-point execution to trap to EL1 when executed from EL0 or EL1. The possible values are:

0bX0 Trap any instruction in EL0 or EL1 that uses registers associated with Advanced SIMD and floating-point execution. The reset value is 0b00.

0b01 Trap any instruction in EL0 that uses registers associated with Advanced SIMD and floating-point execution. Instructions in EL1 are not trapped.

0b11 No instructions are trapped.

This field is RES0 if Advanced SIMD and floating-point are not implemented.

[19:0]

Reserved, RES0.

To access the CPACR_EL1:

```
MRS <Xt>, CPACR_EL1 ; Read CPACR_EL1 into Xt
MSR CPACR_EL1, <Xt> ; Write Xt to CPACR_EL1
```

Register access is encoded as follows:

Table B1-24 CPACR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0001	0000	010

B1.32 Architectural Feature Trap Register, EL2

The CPTR_EL2 characteristics are:

Purpose

Controls trapping to EL2 for accesses to CPACR, Trace functionality and registers associated with Advanced SIMD and floating-point execution. Controls EL2 access to this functionality.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

CPTR_EL2 is a 32-bit register.

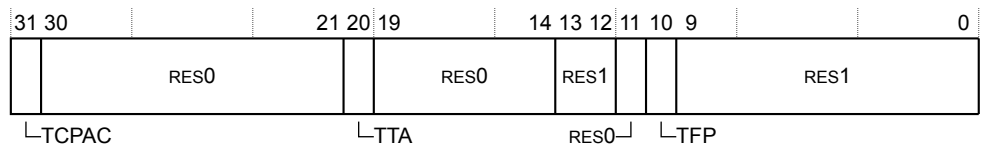


Figure B1-7 CPTR_EL2 bit assignments

TCPAC, [31]

Traps direct access to CPACR from Non-secure EL1 to EL2. The possible values are:

- 0 Access to CPACR is not trapped. This is the reset value.
- 1 Access to CPACR is trapped.

[30:21]

Reserved, RES0.

TTA, [20]

Trap Trace Access.

Not implemented. RES0.

[19:14]

Reserved, RES0.

[13:12]

Reserved, RES1.

[11]

Reserved, RES0.

TFP, [10]

Traps instructions that access registers associated with Advanced SIMD and floating-point execution from a lower exception level to EL2, unless trapped to EL1. The possible values are:

- 0 Instructions are not trapped. This is the reset value if Advanced SIMD and floating-point are implemented.
- 1 Instructions are trapped. This is always the value if Advanced SIMD and floating-point are not implemented.

[9:0]

Reserved, RES1.

To access the CPTR_EL2:

```
MRS <Xt>, CPTR_EL2 ; Read CPTR_EL2 into Xt  
MSR CPTR_EL2, <Xt> ; Write Xt to CPTR_EL2
```

B1.33 Architectural Feature Trap Register, EL3

The CPTR_EL3 characteristics are:

Purpose

Controls trapping to EL3 for accesses to CPACR, Trace functionality and registers associated with Advanced SIMD and floating-point execution. Controls EL3 access to this functionality.

CPTR_EL3 is part of the Security registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

CPTR_EL3 is a 32-bit register.

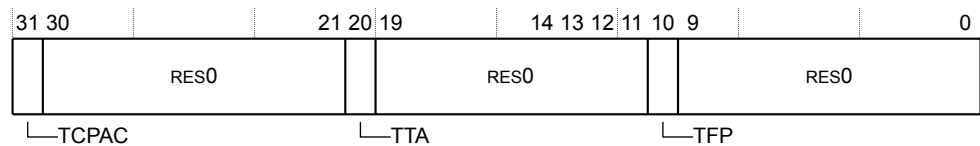


Figure B1-8 CPTR_EL3 bit assignments

TCPAC, [31]

This causes a direct access to the CPACR_EL1 from EL1 or the CPTR_EL2 from EL2 to trap to EL3 unless it is trapped at EL2. The possible values are:

- 0 Does not cause access to the CPACR_EL1 or CPTR_EL2 to be trapped.
- 1 Causes access to the CPACR_EL1 or CPTR_EL2 to be trapped.

[30:21]

Reserved, RES0.

TTA, [20]

Trap Trace Access.

Not implemented. RES0.

[19:11]

Reserved, RES0.

TFP, [10]

This causes instructions that access the registers associated with Advanced SIMD or floating-point execution to trap to EL3 when executed from any exception level, unless trapped to EL1 or EL2. The possible values are:

- 0 Does not cause any instruction to be trapped. This is the reset value if the Advanced SIMD and floating-point support is implemented.
- 1 Causes any instructions that use the registers associated with Advanced SIMD or floating-point execution to be trapped. This is always the value if the Advanced SIMD and floating-point support is not implemented.

[9:0]

Reserved, RES0.

To access the CPTR_EL3:

```
MRS <Xt>, CPTR_EL3 ; Read CPTR_EL3 into Xt  
MSR CPTR_EL3, <Xt> ; Write Xt to CPTR_EL3
```

B1.34 CPU Auxiliary Control Register, EL1

The CPUACTLR_EL1 characteristics are:

Purpose

Provides IMPLEMENTATION DEFINED configuration and control options for the processor. There is one 64-bit CPU Auxiliary Control Register for each core in the processor.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
-	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

The CPU Auxiliary Control Register can be written only when the system is idle. ARM recommends that you write to this register after a powerup reset, before the MMU is enabled, and before any master interface or ACP traffic begins.

Setting many of these bits can cause significantly lower performance on your code. Therefore, it is suggested that you do not modify this register unless directed by ARM.

Configurations

CPUACTLR_EL1 is common to the Secure and Non-secure states.

Attributes

CPUACTLR_EL1 is a 64-bit register.

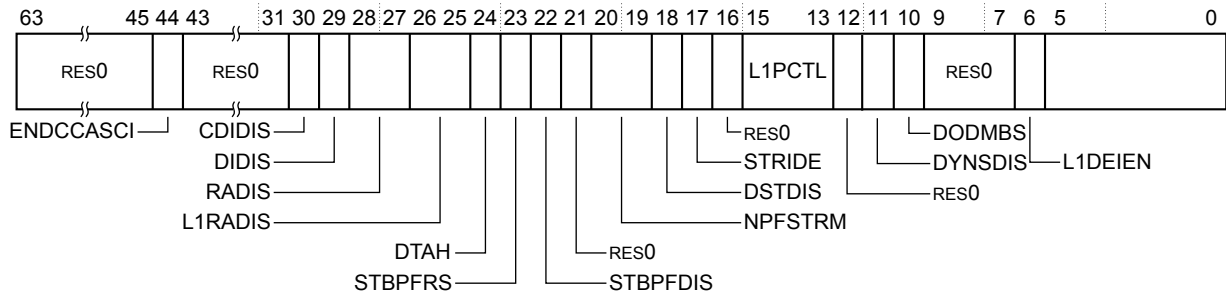


Figure B1-9 CPUACTLR_EL1 bit assignments

[63:45]

Reserved, RES0.

ENDCCASCI, [44]

Enable data cache clean as data cache clean/invalidate. The possible values are:

- 0 Normal behavior, data cache clean operations are unaffected. This is the reset value.
- 1 Executes data cache clean operations as data cache clean and invalidate. The following operations are affected:
 - In AArch64, DC CSW is executed as DC CISW, DC CVAU and DC CVAC are executed as DC CIVAC.

[43:31]

Reserved, RES0.

CDIDIS, [30]

Disable Cryptographic dual issue. The possible values are:

- 0 Enable dual issue of floating-point, Advanced SIMD and Cryptographic instructions. This is the reset value.

- 1 Disable dual issue of floating-point, Advanced SIMD and Cryptographic instructions.

DIDIS, [29]

Disable Dual Issue. The possible values are:

- 0 Enable Dual Issue of instructions. This is the reset value.
- 1 Disable Dual Issue of all instructions.

RADIS, [28:27]

Write streaming no-allocate threshold. The possible values are:

- 0b00 16th consecutive streaming cache line does not allocate in the L1 or L2 cache.
- 0b01 128th consecutive streaming cache line does not allocate in the L1 or L2 cache. This is the reset value.
- 0b10 512th consecutive streaming cache line does not allocate in the L1 or L2 cache.
- 0b11 Disables streaming. All write-allocate lines allocate in the L1 or L2 cache.

L1RADIS, [26:25]

Write streaming no-L1-allocate threshold. The possible values are:

- 0b00 4th consecutive streaming cache line does not allocate in the L1 cache. This is the reset value.
- 0b01 64th consecutive streaming cache line does not allocate in the L1 cache.
- 0b10 128th consecutive streaming cache line does not allocate in the L1 cache.
- 0b11 Disables streaming. All write-allocate lines allocate in the L1 cache.

DTAH, [24]

Disable transient and no-read-allocate hints for loads. The possible values are:

- 0 Normal operation.
- 1 Transient and no-read-allocate hints in the MAIR are ignored and treated the same as non-transient, read-allocate types for loads. The LDNP instruction in AArch64 behaves the same as the equivalent LDP instruction. This is the reset value.

STBPFRS, [23]

Disable ReadUnique request for prefetch streams initiated by STB accesses:

- 0 ReadUnique used for prefetch streams initiated from STB accesses. This is the reset value.
- 1 ReadShared used for prefetch streams initiated from STB accesses.

STBPFDIS, [22]

Disable prefetch streams initiated from STB accesses:

- 0 Enable Prefetch streams initiated from STB accesses. This is the reset value.
- 1 Disable Prefetch streams initiated from STB accesses.

[21]

Reserved, RES0.

NPFSTRM, [20:19]

Number of independent data prefetch streams. The possible values are:

- 0b00 1 stream.
- 0b01 2 streams. This is the reset value.
- 0b10 3 streams.
- 0b11 4 streams.

DSTDIS, [18]

Enable device split throttle. The possible values are:

- 0 Device split throttle disabled.
- 1 Device split throttle enabled. This is the reset value.

STRIDE, [17]

Configure the sequence length that triggers data prefetch streams. The possible values are:

- 0 2 linefills to consecutive cache lines triggers prefetch. This is the reset value.
- 1 3 linefills to consecutive cache lines triggers prefetch.

In both configurations, Three linefills with a fixed stride pattern are required to trigger prefetch, if the stride spans more than one cache line.

[16]

Reserved, RES0.

L1PCTL, [15:13]

L1 Data prefetch control. The value of the this field determines the maximum number of outstanding data prefetches allowed in the L1 memory system, excluding those generated by software load or PLD instructions. The possible values are:

- 0b000 Prefetch disabled.
- 0b001 1 outstanding prefetch allowed.
- 0b010 2 outstanding prefetches allowed.
- 0b011 3 outstanding prefetches allowed.
- 0b100 4 outstanding prefetches allowed.
- 0b101 5 outstanding prefetches allowed. This is the reset value.
- 0b110 6 outstanding prefetches allowed.
- 0b111 8 outstanding prefetches allowed.

[12:11]

Reserved, RES0.

DODMBS, [10]

Disable optimized Data Memory Barrier behavior. The possible values are:

- 0 Enable optimized Data Memory Barrier behavior. This is the reset value.
- 1 Disable optimized Data Memory Barrier behavior.

[9:7]

Reserved, RES0.

L1DEIEN, [6]

L1 D-cache data RAM error injection enable. The possible values are:

- 0 Normal behavior, errors are not injected. This is the reset value.
- 1 Double-bit errors are injected on all writes to the L1 D-cache data RAMs for the first word of each 32-byte region.

[5:0]

Reserved, RES0.

To access the CPUACTLR_EL1:

```
MRS <Xt>, S3_1_C15_C2_0 ; Read EL1 CPU Auxiliary Control Register
MSR S3_1_C15_C2_0, <Xt> ; Write EL1 CPU Auxiliary Control Register
```

Register access is encoded as follows:

Table B1-25 CPUACTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0010	000

B1.35 CPU Extended Control Register, EL1

The CPUECTLR_EL1 characteristics are:

Purpose

Provides additional IMPLEMENTATION DEFINED configuration and control options for the processor.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

The CPUECTLR_EL1 can be written dynamically.

The CPUECTLR_EL1 is write accessible in EL1 if ACTLR_EL3.CPUECTLR is 1 and ACTLR_EL2.CPUECTLR is 1, or ACTLR_EL3.CPUECTLR is 1 and SCR.NS is 0.

The CPUECTLR_EL1 is write accessible in EL2 if ACTLR_EL3.CPUECTLR is 1.

Configurations

There are no configuration notes.

Attributes

CPUECTLR_EL1 is a 64-bit register.

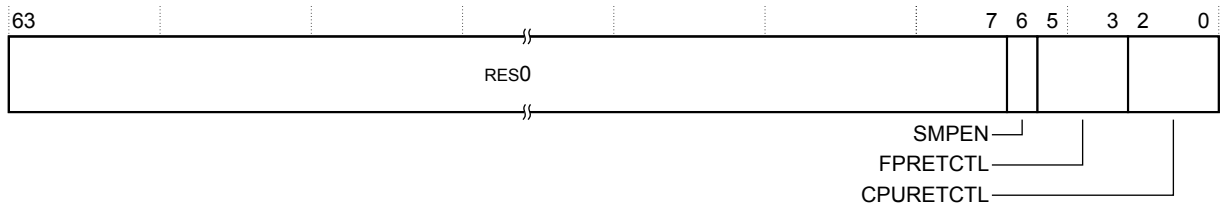


Figure B1-10 CPUECTLR_EL1 bit assignments

[63:7]

Reserved, RES0.

SMPEN, [6]

Enable hardware management of data coherency with other cores in the cluster. The possible values are:

- 0 Disables data coherency with other cores in the cluster. This is the reset value.
- 1 Enables data coherency with other cores in the cluster.

Set the SMPEN bit before enabling the caches, even if there is only one core in the system.

[5:3]

Advanced SIMD and floating-point retention control. The possible values are:

- 0b000 Disable the retention circuit. This is the reset value.
- 0b001 2 Architectural Timer ticks are required before retention entry.
- 0b010 8 Architectural Timer ticks are required before retention entry.
- 0b011 32 Architectural Timer ticks are required before retention entry.
- 0b100 64 Architectural Timer ticks are required before retention entry.
- 0b101 128 Architectural Timer ticks are required before retention entry.
- 0b110 256 Architectural Timer ticks are required before retention entry.
- 0b111 512 Architectural Timer ticks are required before retention entry.

This field is present only if the Advanced SIMD and floating-point support is implemented. Otherwise, it is RES0.

[2:0]

CPU retention control. The possible values are:

- 0b000 Disable the retention circuit. This is the reset value.
- 0b001 2 Architectural Timer ticks are required before retention entry.
- 0b010 8 Architectural Timer ticks are required before retention entry.
- 0b011 32 Architectural Timer ticks are required before retention entry.
- 0b100 64 Architectural Timer ticks are required before retention entry.
- 0b101 128 Architectural Timer ticks are required before retention entry.
- 0b110 256 Architectural Timer ticks are required before retention entry.
- 0b111 512 Architectural Timer ticks are required before retention entry.

To access the CPUECTLR_EL1:

MRS <Xt>, S3_1_C15_C2_1; Read EL1 CPU Extended Control Register
 MSR S3_1_C15_C2_1, <Xt>; Write EL1 CPU Extended Control Register

Register access is encoded as follows:

Table B1-26 CPUECTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0010	001

B1.36 CPU Memory Error Syndrome Register, EL1

The CPUMERRSR_EL1 characteristics are:

Purpose

Holds ECC errors on the:

- L1 data RAMs.
- L1 tag RAMs.
- L1 dirty RAMs.
- TLB RAMs.

This register is used for recording ECC errors on all processor RAMs.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

A write of any value to the register updates the register to 0x0000000000000000.

Attributes

CPUMERRSR_EL1 is a 64-bit register.

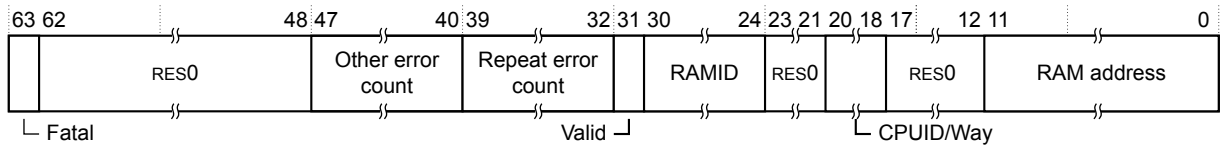


Figure B1-11 CPUMERRSR_EL1 bit assignments

Fatal, [63]

Fatal bit. This bit is set to 1 on the first memory error that caused a data abort. It is a sticky bit so that after it is set, it remains set until the register is written.

The reset value is 0.

[62:48]

Reserved, RES0.

Other error count, [47:40]

This field is set to 0 on the first memory error and is incremented on any memory error that does not match the RAMID and Bank/Way information in this register while the sticky Valid bit is set.

The reset value is 0.

Repeat error count, [39:32]

This field is set to 0 on the first memory error and is incremented on any memory error that exactly matches the RAMID and Bank/Way information in this register while the sticky Valid bit is set.

The reset value is 0.

Valid, [31]

Valid bit. This bit is set to 1 on the first memory error. It is a sticky bit so that after it is set, it remains set until the register is written.

The reset value is 0.

RAMID, [30:24]

RAM Identifier. Indicates the RAM in which the first memory error. The possible values are:

- 0x00 L1 Instruction tag RAM.
- 0x01 L1 Instruction data RAM.
- 0x08 L1 Data tag RAM.
- 0x09 L1 Data data RAM.
- 0x0A L1 Data dirty RAM.
- 0x18 TLB RAM.

[23:21]

Reserved, RES0.

CPUID/Way, [20:18]

Indicates the RAM where the first memory error occurred.

L1 I-tag RAM

- 0x0 Way 0
- 0x1 Way 1
- 0x2-0x7 Unused

L1 I-data RAM

- 0x0 Bank 0
- 0x1 Bank 1
- 0x2-0x7 Unused

TLB RAM

- 0x0 Way 0
- 0x1 Way 1
- 0x2-0x7 Unused

L1 D-dirty RAM

- 0x0 Dirty RAM
- 0x1-0x7 Unused

L1 D-tag RAM

- 0x0 Way 0
- 0x1 Way 1
- 0x2 Way 2
- 0x3 Way 3
- 0x4-0x7 Unused

L1 D-data RAM

- 0x0 Bank0
- 0x1 Bank1
- 0x2 Bank2
- 0x3 Bank3
- ...

0x7 Bank7

[17:12]

Reserved, RES0.

RAM address, [11:0]

Indicates the index address of the first memory error.

- A fatal error results in the RAMID, Way, and RAM address recording the fatal error, even if the sticky bit is set.
- Only L1 Data data and L1 Data dirty RAMs can signal fatal errors, because all other RAM instances are protected only by parity.
- If two or more memory errors in the same RAM occur in the same cycle, only one error is reported.
- If two or more first memory error events from different RAMs occur in the same cycle, one of the errors is selected arbitrarily.
- If two or more memory error events from different RAMs, that do not match the RAMID, Way, and index information in this register while the sticky Valid bit is set, occur in the same cycle, then the Other error count field is incremented only by one.

To access the CPUMERRSR_EL1:

```
MRS <Xt>, S3_1_c15_c2_2 ; Read CPUMERRSR into Xt
MSR S3_1_c15_c2_2, <Xt> ; Write Xt to CPUMERRSR
```

Register access is encoded as follows:

Table B1-27 CPUMERRSR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0010	010

B1.37 Cache Type Register, EL0

The CTR_EL0 characteristics are:

Purpose

Provides information about the architecture of the caches.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
Config	RO	RO	RO	RO	RO

This register is accessible at EL0 when SCTLR_EL1.UCT is set to 1.

Configurations

There are no configuration notes.

Attributes

CTR_EL0 is a 32-bit register.

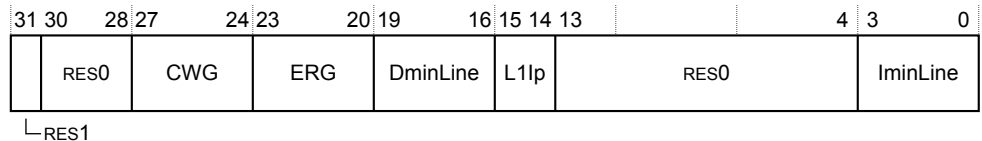


Figure B1-12 CTR_EL0 bit assignments

[31]

Reserved, RES1.

[30:28]

Reserved, RES0.

CWG, [27:24]

Cache Write-Back granule. \log_2 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:

0x4 Cache Write-Back granule size is 16 words.

ERG, [23:20]

Exclusives Reservation Granule. \log_2 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:

0x4 Exclusive reservation granule size is 16 words.

DminLine, [19:16]

\log_2 of the number of words in the smallest cache line of all the data and unified caches that the processor controls:

0x4 Smallest data cache line size is 16 words.

L1Ip, [15:14]

L1 Instruction cache policy. Indicates the indexing and tagging policy for the L1 Instruction cache:

0b10 *Virtually Indexed Physically Tagged (VIPT)*.

[13:4]

Reserved, RES0.

IminLine, [3:0]

\log_2 of the number of words in the smallest cache line of all the instruction caches that the processor controls.

0x4 Smallest instruction cache line size is 16 words.

To access the CTR_EL0:

```
MRS <Xt>, CTR_EL0 ; Read CTR_EL0 into Xt
```

Register access is encoded as follows:

Table B1-28 CTR_EL0 access encoding

op0	op1	CRn	CRm	op2
11	011	0000	0000	001

B1.38 Data Cache Zero ID Register, EL0

The DCZID_EL0 characteristics are:

Purpose

Indicates the block size written with byte values of zero by the DC ZVA (Cache Zero by Address), system instruction.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
RO	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

DCZID_EL0 is a 32-bit register.

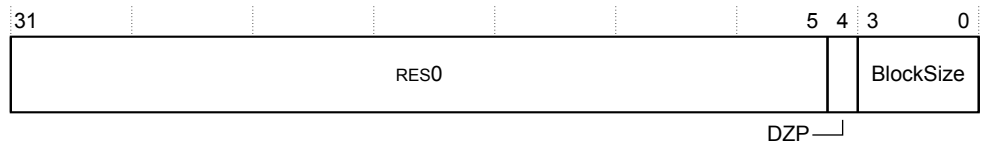


Figure B1-13 DCZID_EL0 bit assignments

[32:5]

Reserved, RES0.

DZP, [4]

Prohibit the DC ZVA instruction:

- 0 DC ZVA instruction permitted.
- 1 DC ZVA instruction is prohibited.

BlockSize, [3:0]

Log2 of the block size in words:

0b0100 The block size is 16 words.

To access the DCZID_EL0:

```
MRS <Xt>, DCZID_EL0 ; Read DCZID_EL0 into Xt
```

Register access is encoded as follows:

Table B1-29 DCZID_EL0 access encoding

op0	op1	CRn	CRm	op2
11	011	0000	0000	111

B1.39 Exception Syndrome Register, EL1

The ESR_EL1 characteristics are:

Purpose

Holds syndrome information for an exception taken to EL1.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

ESR_EL1 is a 32-bit register.

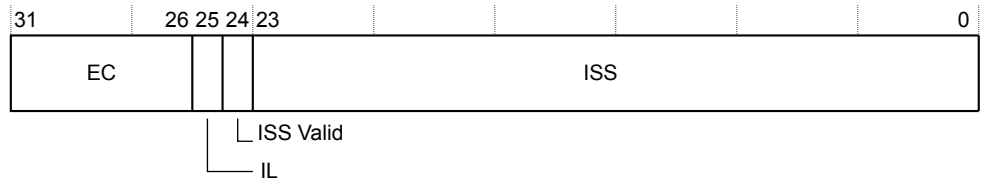


Figure B1-14 ESR_EL1 bit assignments

EC, [31:26]

Exception Class. Indicates the reason for the exception that this register holds information about.

IL, [25]

Instruction Length for synchronous exceptions. The possible values are:

- 0 16-bit.
- 1 32-bit.

This field is 1 for the SError interrupt, instruction aborts, misaligned PC, Stack pointer misalignment, data aborts for which the ISV bit is 0, exceptions caused by an illegal instruction set state, and exceptions using the $0x00$ Exception Class.

ISS Valid, [24]

Syndrome valid. The possible values are:

- 0 ISS not valid, ISS is RES0.
- 1 ISS valid.

ISS, [23:0]

Syndrome information.

When the EC field is $0x2F$, indicating an SError interrupt has occurred, the ISS field contents are IMPLEMENTATION DEFINED.

Table B1-30 ISS field contents for the Cortex-A34 processor

ISS[23:22]	ISS[1:0]	Description
0b00	0b00	DECERR on external access
0b00	0b01	Double-bit error detected on dirty line in L2 cache

Table B1-30 ISS field contents for the Cortex-A34 processor (continued)

ISS[23:22]	ISS[1:0]	Description
0b00	0b10	SLVERR on external access
0b01	0b00	nSEI, or nVSEI in a guest OS, asserted
0b01	0b01	nREI asserted

To access the ESR_EL1:

MRS <Xt>, ESR_EL1 ; Read EL1 Exception Syndrome Register
 MSR ESR_EL1, <Xt> ; Write EL1 Exception Syndrome Register

Register access is encoded as follows:

Table B1-31 ESR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0101	0010	000

B1.40 Exception Syndrome Register, EL2

The ESR_EL2 characteristics are:

Purpose

Holds syndrome information for an exception taken to EL2.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

ESR_EL2 is a 32-bit register.

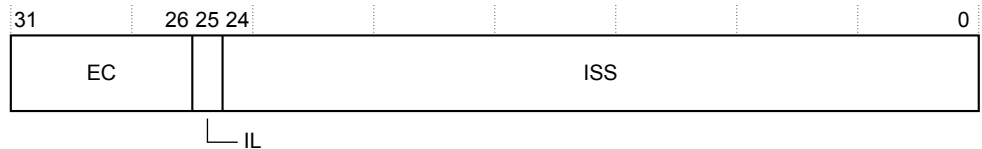


Figure B1-15 ESR_EL2 bit assignments

EC, [31:26]

Exception Class. Indicates the reason for the exception that this register holds information about.

IL, [25]

Instruction Length for synchronous exceptions. The possible values are:

- 0 16-bit.
- 1 32-bit.

ISS, [24:0]

Syndrome information.

When the EC field is 0x2F, indicating an SError interrupt has occurred, the ISS field contents are IMPLEMENTATION DEFINED.

Table B1-32 ISS field contents for the Cortex-A34 processor

ISS[23:22]	ISS[1:0]	Description
0b00	0b00	DECERR on external access
0b00	0b01	Double-bit error detected on dirty line in L2 cache
0b00	0b10	SLVERR on external access
0b01	0b00	nSEI, or nVSEI in a guest OS, asserted
0b01	0b01	nREI asserted

To access the ESR_EL2:

MRS <Xt>, ESR_EL2 ; Read EL1 Exception Syndrome Register
 MSR ESR_EL2, <Xt> ; Write EL1 Exception Syndrome Register

Register access is encoded as follows:

Table B1-33 ESR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0101	0010	000

B1.41 Exception Syndrome Register, EL3

The ESR_EL3 characteristics are:

Purpose

Holds syndrome information for an exception taken to EL3.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

ESR_EL3 is a 32-bit register.

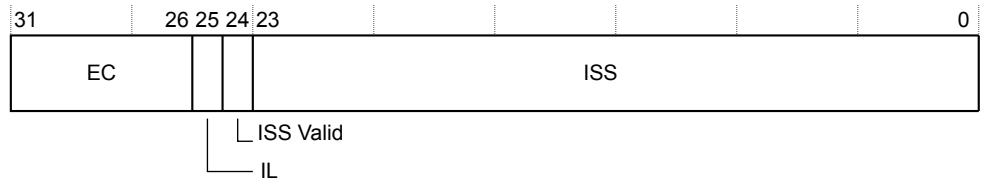


Figure B1-16 ESR_EL3 bit assignments

EC, [31:26]

Exception Class. Indicates the reason for the exception that this register holds information about.

IL, [25]

Instruction Length for synchronous exceptions. The possible values are:

- 0 16-bit.
- 1 32-bit.

This field is 1 for the SError interrupt, instruction aborts, misaligned PC, Stack pointer misalignment, data aborts for which the ISV bit is 0, exceptions caused by an illegal instruction set state, and exceptions using the 0x0 Exception Class.

ISS Valid, [24]

Syndrome valid. The possible values are:

- 0 ISS not valid, ISS is RES0.
- 1 ISS valid.

ISS, [23:0]

Syndrome information.

When the EC field is 0x2F, indicating an SError interrupt has occurred, the ISS field contents are IMPLEMENTATION DEFINED.

Table B1-34 ISS field contents for the Cortex-A34 processor

ISS[23:22]	ISS[1:0]	Description
0b00	0b00	DECERR on external access
0b00	0b01	Double-bit error detected on dirty line in L2 cache

Table B1-34 ISS field contents for the Cortex-A34 processor (continued)

ISS[23:22]	ISS[1:0]	Description
0b00	0b10	SLVERR on external access
0b01	0b00	nSEI , or nVSEI in a guest OS, asserted
0b01	0b01	nREI asserted

To access the ESR_EL3:

MRS <Xt>, ESR_EL3 ; Read EL3 Exception Syndrome Register
 MSR ESR_EL3, <Xt> ; Write EL3 Exception Syndrome Register

Register access is encoded as follows:

Table B1-35 ESR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0101	0010	000

B1.42 Fault Address Register, EL1

The FAR_EL1 characteristics are:

Purpose

Holds the faulting Virtual Address for all synchronous instruction or data aborts, or exceptions from a misaligned PC or a Watchpoint debug event, taken to EL1.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

FAR_EL1 is a 64-bit register.

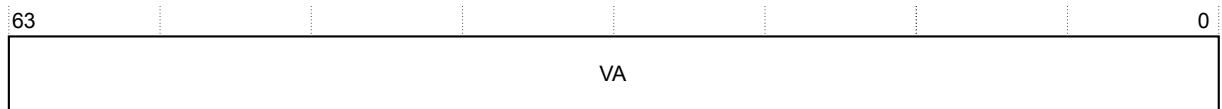


Figure B1-17 FAR_EL1 bit assignments

VA, [63:0]

The faulting Virtual Address for all synchronous instruction or data aborts, or an exception from a misaligned PC, taken in EL1.

If a memory fault that sets the FAR is generated from one of the data cache instructions, this field holds the address specified in the register argument of the instruction.

To access the FAR_EL1:

```
MRS <Xt>, FAR_EL1 ; Read EL1 Fault Address Register
MSR FAR_EL1, <Xt> ; Write EL1 Fault Address Register
```

Register access is encoded as follows:

Table B1-36 FAR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0110	0000	000

B1.43 Fault Address Register, EL2

The FAR_EL2 characteristics are:

Purpose

Holds the faulting Virtual Address for all synchronous instruction or data aborts, or exceptions from a misaligned PC or a Watchpoint debug event, taken to EL2.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

FAR_EL2 is a 64-bit register.

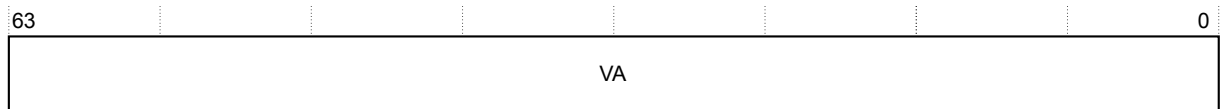


Figure B1-18 FAR_EL2 bit assignments

VA, [63:0]

The faulting Virtual Address for all synchronous instruction or data aborts, or an exception from a misaligned PC, taken in EL2.

If a memory fault that sets the FAR is generated from one of the data cache instructions, this field holds the address specified in the register argument of the instruction.

To access the FAR_EL2:

```
MRS <Xt>, FAR_EL2 ; Read EL2 Fault Address Register
MSR FAR_EL2, <Xt> ; Write EL2 Fault Address Register
```

Register access is encoded as follows:

Table B1-37 FAR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0110	0000	000

B1.44 Fault Address Register, EL3

The FAR_EL3 characteristics are:

Purpose

Holds the faulting Virtual Address for all synchronous instruction or data aborts, or exceptions from a misaligned PC, taken to EL3.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There is no additional configuration data for FAR_EL3.

Attributes

FAR_EL3 is a 64-bit register.

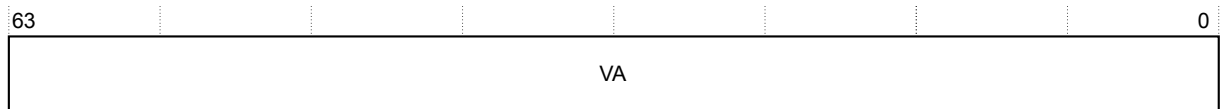


Figure B1-19 FAR_EL3 bit assignments

VA, [63:0]

The faulting Virtual Address for all synchronous instruction or data aborts, or an exception from a misaligned PC, taken in EL3.

If a memory fault that sets the FAR is generated from one of the data cache instructions, this field holds the address specified in the register argument of the instruction.

To access the FAR_EL3:

```
MRS <Xt>, FAR_EL3 ; Read EL3 Fault Address Register
MSR FAR_EL3, <Xt> ; Write EL3 Fault Address Register
```

Register access is encoded as follows:

Table B1-38 FAR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0110	0000	000

B1.45 Hyp Auxiliary Configuration Register, EL2

HACR_EL2

The processor does not implement HACR_EL2. This register is always RES0.

B1.46 Hypervisor Configuration Register, EL2

The HCR_EL2 characteristics are:

Purpose

Provides configuration control for virtualization, including whether various Non-secure operations are trapped to EL2.

HCR_EL2 is part of the Hypervisor and virtualization registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

HCR_EL2 is a 64-bit register.

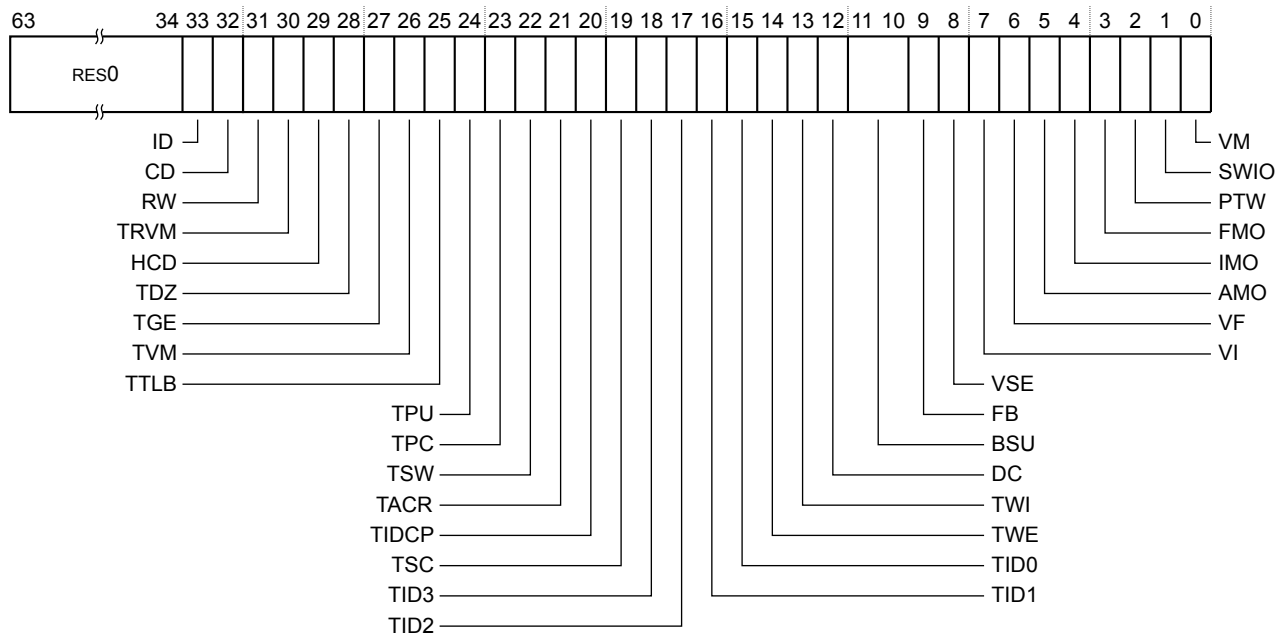


Figure B1-20 HCR_EL2 bit assignments

[63:34]

Reserved, RES0.

ID, [32]

Disables stage 2 instruction cache. When HCR_EL2.VM is 1, this forces all stage 2 translations for instruction accesses to Normal memory to be Non-cacheable for the EL1/EL0 translation regimes. The possible values are:

- 0 Has no effect on stage 2 EL1/EL0 translation regime for instruction accesses. This is the reset value.
- 1 Forces all stage 2 translations for instruction accesses to Normal memory to be Non-cacheable for the EL1/EL0 translation regime.

CD, [31]

Disables stage 2 data cache. When HCR_EL2.VM is 1, this forces all stage 2 translations for data accesses and translation table walks to Normal memory to be Non-cacheable for the EL1/EL0 translation regimes. The possible values are:

- 0 Has no effect on stage 2 EL1/EL0 translation regime for data access or translation table walks. This is the reset value.
- 1 Forces all stage 2 translations for data accesses and translation table walks to Normal memory to be Non-cacheable for the EL1/EL0 translation regime.

RW, [31]

RAO/WI

TRVM, [30]

Trap reads of Virtual Memory controls. The possible values are:

- 0 Non-secure EL1 reads are not trapped. This is the reset value.
- 1 Non-secure EL1 reads are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

HCD, [29]

Reserved, RES0.

TDZ, [28]

Traps DC ZVA instruction. The possible values are:

- 0 DC ZVA instruction is not trapped. This is the reset value.
- 1 DC ZVA instruction is trapped to EL2 when executed in Non-secure EL1 or EL0.

TGE, [27]

Traps general exceptions. If this bit is set, and SCR_EL3.NS is set, then:

- All Non-secure EL1 exceptions are routed to EL2.
- For Non-secure EL1, the SCTLR_EL1.M bit is treated as 0 regardless of its actual state other than the purpose of reading the bit.
- The HCR_EL2.FMO, HCR_EL2.IMO, and HCR_EL2.AMO bits are treated as 1 regardless of their actual state other than for the purpose of reading the bits.
- All virtual interrupts are disabled.
- Any implementation defined mechanisms for signaling virtual interrupts are disabled.
- An exception return to Non-secure EL1 is treated as an illegal exception return.

TVM, [26]

Trap virtual memory controls. The possible values are:

- 0 Non-secure EL1 writes are not trapped. This is the reset value.
- 1 Non-secure EL1 writes are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TTLB, [25]

Traps TLB maintenance instructions. The possible values are:

- 0 Non-secure EL1 TLB maintenance instructions are not trapped. This is the reset value.
- 1 TLB maintenance instructions executed from Non-secure EL1 that are not UNDEFINED are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TPU, [24]

Traps cache maintenance instructions to *Point of Unification* (POU). The possible values are:

- 0 Cache maintenance instructions are not trapped. This is the reset value.
- 1 Cache maintenance instructions to the POU executed from Non-secure EL1 or EL0 that are not UNDEFINED are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TPC, [23]

Traps data or unified cache maintenance instructions to *Point of Coherency* (POC). The possible values are:

- 0 Data or unified cache maintenance instructions are not trapped. This is the reset value.
- 1 Data or unified cache maintenance instructions by address to the POC executed from Non-secure EL1 or EL0 that are not UNDEFINED are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TSW, [22]

Traps data or unified cache maintenance instructions by Set or Way. The possible values are:

- 0 Data or unified cache maintenance instructions are not trapped. This is the reset value.
- 1 Data or unified cache maintenance instructions by Set or Way executed from Non-secure EL1 that are not UNDEFINED are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TACR, [21]

Traps Auxiliary Control registers. The possible values are:

- 0 Accesses to Auxiliary Control registers are not trapped. This is the reset value.
- 1 Accesses to ACTLR_EL1 in the AArch64 state from Non-secure EL1 are trapped to EL2.

TIDCP, [20]

Trap Implementation Dependent functionality. When 1, this causes accesses to the following instruction set space executed from Non-secure EL1 to be trapped to EL2:

AArch64 Reserved control space for IMPLEMENTATION DEFINED functionality.

Accesses from EL0 are UNDEFINED. The reset value is 0.

TSC, [19]

Traps SMC instruction. The possible values are:

- 0 SMC instruction in not trapped. This is the reset value.
- 1 SMC instruction executed in Non-secure EL1 is trapped to EL2.

TID3, [18]

Traps ID group 3 registers. The possible values are:

- 0 ID group 3 register accesses are not trapped. This is the reset value.
- 1 Reads to ID group 3 registers executed from Non-secure EL1 are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TID2, [17]

Traps ID group 2 registers. The possible values are:

- 0 ID group 2 register accesses are not trapped. This is the reset value.
- 1 Reads to ID group 2 registers and writes to CSSELR and CSSELR_EL1 executed from Non-secure EL1 or EL0, if not UNDEFINED, are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TID1, [16]

Traps ID group 1 registers. The possible values are:

- 0 ID group 1 register accesses are not trapped. This is the reset value.
- 1 Reads to ID group 1 registers executed from Non-secure EL1 are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TID0, [15]

Traps ID group 0 registers. The possible values are:

- 0 ID group 0 register accesses are not trapped. This is the reset value.
- 1 Reads to ID group 0 registers executed from Non-secure EL1 are trapped to EL2.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the registers covered by this setting.

TWE, [14]

Traps WFE instruction if it would cause suspension of execution. For example, if there is no pending WFE event. The possible values are:

- 0 WFE instruction is not trapped. This is the reset value.
- 1 WFE instruction executed in Non-secure EL1 or EL0 is trapped to EL2.

TWI, [13]

Traps WFI instruction if it causes suspension of execution. For example, if there is no pending WFI event. The possible values are:

- 0 WFI instruction is not trapped. This is the reset value.
- 1 WFI instruction executed in Non-secure EL1 or EL0 is trapped to EL2.

DC, [12]

Default cacheable. When this bit is set it causes:

- SCTLR_EL1.M to behave as 0 for all purposes other than reading the bit.
- HCR_EL2.VM to behave as 1 for all purposes other than reading the bit.

The memory type produced by the first stage of translation in Non-secure EL1 and EL0 is Non-Shareable, Inner Write-Back Write-Allocate, Outer Write-Back Write-Allocate. The reset value is 0.

BSU, [11:10]

Barrier shareability upgrade. Determines the minimum shareability domain that is supplied to any barrier executed from Non-secure EL1 or EL0. The possible values are:

- 0b00 No effect. This is the reset value.
- 0b01 Inner Shareable.
- 0b10 Outer Shareable.
- 0b11 Full system.

This value is combined with the specified level of the barrier held in its instruction, according to the algorithm for combining shareability attributes.

FB, [9]

Forces broadcast. The possible values are:

- 0 Instructions are not broadcast. This is the reset value.
- 1 Forces instruction broadcast within Inner Shareable domain when executing from Non-secure EL1.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for the instructions covered by this setting.

VSE, [8]

Virtual System Error/Asynchronous Abort. The possible values are:

- 0 Virtual System Error/Asynchronous Abort is not pending by this mechanism. This is the reset value.
- 1 Virtual System Error/Asynchronous Abort is pending by this mechanism.

The virtual System Error/Asynchronous Abort is enabled only when the HCR_EL2.AMO bit is set.

VI, [7]

Virtual IRQ interrupt. The possible values are:

- 0 Virtual IRQ is not pending by this mechanism. This is the reset value.
- 1 Virtual IRQ is pending by this mechanism.

The virtual IRQ is enabled only when the HCR_EL2.IMO bit is set.

VF, [6]

Virtual FIQ interrupt. The possible values are:

- 0 Virtual FIQ is not pending by this mechanism. This is the reset value.
- 1 Virtual FIQ is pending by this mechanism.

The virtual FIQ is enabled only when the HCR_EL2.FMO bit is set.

AMO, [5]

Asynchronous abort and error interrupt routing. The possible values are:

- 0 Asynchronous external Aborts and SError Interrupts while executing at exception levels lower than EL2 are not taken at EL2. Virtual System Error/Asynchronous Abort is disabled. This is the reset value.
- 1 Asynchronous external Aborts and SError Interrupts while executing at EL2 or lower are taken in EL2 unless routed by SCTLR_EL3.EA bit to EL3. Virtual System Error/Asynchronous Abort is enabled.

IMO, [4]

Physical IRQ routing. The possible values are:

- 0 Physical IRQ while executing at exception levels lower than EL2 are not taken at EL2. Virtual IRQ interrupt is disabled. This is the reset value.
- 1 Physical IRQ while executing at EL2 or lower are taken in EL2 unless routed by SCTLR_EL3.IRQ bit to EL3. Virtual IRQ interrupt is enabled.

FMO, [3]

Physical FIQ routing. The possible values are:

- 0 Physical FIQ while executing at exception levels lower than EL2 are not taken at EL2. Virtual FIQ interrupt is disabled. This is the reset value.
- 1 Physical FIQ while executing at EL2 or lower are taken in EL2 unless routed by SCTLR_EL3.FIQ bit to EL3. Virtual FIQ interrupt is enabled.

PTW, [2]

Protected Table Walk. When this bit is set, if the stage 2 translation of a translation table access, made as part of a stage 1 translation table walk at EL0 or EL1, maps to Device memory, the access is faulted as a stage 2 Permission fault. The reset value is 0.

SWIO, [1]

Set/Way Invalidation Override. Non-secure EL1 execution of the data cache invalidate by set/way instruction is treated as data cache clean and invalidate by set/way. When this bit is set, DC ISW is treated as DC CISW.

This bit is RES1.

VM, [0]

Enables second stage of translation. The possible values are:

- 0 Disables second stage translation. This is the reset value.
- 1 Enables second stage translation for execution in Non-secure EL1 and EL0.

To access the HCR_EL2:

```
MRS <Xt>, HCR_EL2 ; Read HCR_EL2 into Xt  
MSR HCR_EL2, <Xt> ; Write Xt to HCR_EL2
```

Register access is encoded as follows:

Table B1-39 HCR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0001	0001	000

B1.47 Hypervisor IPA Fault Address Register, EL2

The HPFAR_EL2 characteristics are:

Purpose

Holds the faulting IPA for some aborts on a stage 2 translation taken to EL2.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

HPFAR_EL2 is a 64-bit register.

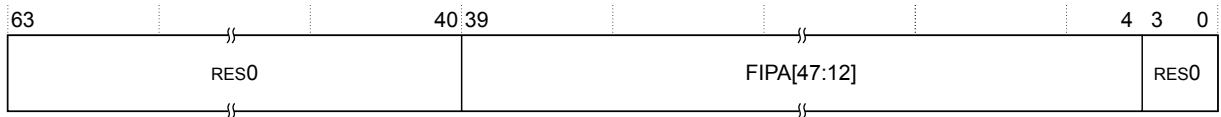


Figure B1-21 HPFAR_EL2 bit assignments

[63:40]

Reserved, RES0.

FIPA[47:12], [39:4]

Bits [47:12] of the faulting intermediate physical address. The equivalent upper bits in this field are RES0.

[3:0]

Reserved, RES0.

To access the HPFAR_EL:

MRS <Xt>, HPFAR_EL2 ; Read EL2 Fault Address Register
 MSR HPFAR_EL2, <Xt> ; Write EL2 Fault Address Register

Register access is encoded as follows:

Table B1-40 HPFR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0110	0000	100

B1.48 Hyp System Trap Register, EL2

HSTR_EL2

This register is always RES0.

B1.49 AArch64 Debug Feature Register 0, EL1

The ID_AA64DFR0_EL1 characteristics are:

Purpose

Provides top level information of the debug system in the AArch64 Execution state.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

ID_AA64DFR0_EL1 is architecturally mapped to external register EDDFR.

Attributes

ID_AA64DFR0_EL1 is a 64-bit register.

63	}}	32:31	28:27	24:23	20:19	16:15	12:11	8:7	4:3	0
	}}	RES0	CTX_CMPs	RES0	WRPs	RES0	BRPs	PMUver	Tracever	Debugger
	}}									

Figure B1-22 ID_AA64DFR0_EL1 bit assignments

[63:32]

Reserved, RES0.

CTX_CMPs, [31:28]

Number of breakpoints that are context-aware, minus 1. These are the highest numbered breakpoints:

0b0001 Two breakpoints are context-aware.

[27:24]

Reserved, RES0.

WRPs, [23:20]

The number of watchpoints minus 1:

0b0011 Four watchpoints.

[19:16]

Reserved, RES0.

BRPs, [15:12]

The number of breakpoints minus 1:

0b0101 Six breakpoints.

PMUver, [11:8]

Performance Monitors Extension version.

0b0001 Performance monitor system registers implemented, PMUv3.

Tracever, [7:4]

Trace extension:

0b0000 Trace system registers not implemented.

Debugger, [3:0]

Debug architecture version:

0b0110 ARMv8-A debug architecture implemented.

To access the ID_AA64DFR0_EL1:

```
MRS <Xt>, ID_AA64DFR0_EL1 ; Read ID_AA64DFR0_EL1 into Xt
```

Register access is encoded as follows:

Table B1-41 ID_AA64DFR0_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0101	000

The EDDFR can be accessed through the external debug interface, offset 0xD28.

B1.50 AArch64 Instruction Set Attribute Register 0, EL1

The ID_AA64ISAR0_EL1 characteristics are:

Purpose

Provides information about the optional cryptographic instructions that the processor can support.

The optional Cryptographic engine is not included in the base product of the processor. ARM requires licensees to have contractual rights to obtain the Cortex-A34 Cryptographic engine.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

ID_AA64ISAR0_EL1 is a 64-bit register.

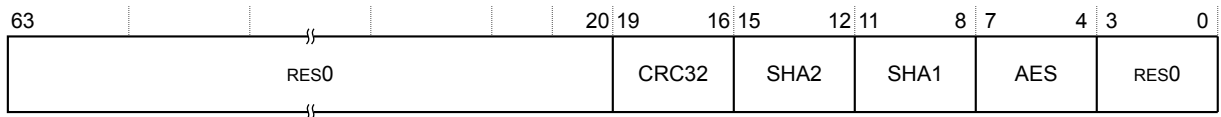


Figure B1-23 ID_AA64ISAR0_EL1 bit assignments

[63:20]

Reserved, RES0.

CRC32, [19:16]

Indicates whether CRC32 instructions are implemented.

0x1 CRC32 instructions are implemented.

SHA2, [15:12]

Indicates whether SHA2 instructions are implemented. The possible values are:

0b0000 No SHA2 instructions implemented. This is the value if the implementation does not include the Cryptographic Extension, or if it is disabled.

0b0001 SHA256H, SHA256H2, SHA256U0, and SHA256U1 implemented. This is the value if the implementation includes the Cryptographic Extension.

All other values reserved.

SHA1, [11:8]

Indicates whether SHA1 instructions are implemented. The possible values are:

0b0000 No SHA1 instructions implemented. This is the value if the implementation does not include the Cryptographic Extension.

0b0001 SHA1C, SHA1P, SHA1M, SHA1SU0, and SHA1SU1 implemented. This is the value if the implementation includes the Cryptographic Extension.

All other values reserved.

AES, [7:4]

Indicates whether AES instructions are implemented. The possible values are:

0b0000 No AES instructions implemented. This is the value if the implementation does not include the Cryptographic Extension.

0b0010 AESE, AESD, AESMC, and AESIMC implemented, plus PMULL and PMULL2 instructions operating on 64-bit data. This is the value if the implementation includes the Cryptographic Extension.

All other values reserved.

[3:0]

Reserved, RES0.

To access the ID_AA64ISAR0_EL1:

```
MRS <Xt>, ID_AA64ISAR0_EL1 ; Read ID_AA64ISAR0_EL1 into Xt
```

Register access is encoded as follows:

Table B1-42 ID_AA64ISAR0_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0110	000

B1.51 AArch64 Processor Feature Register 0, EL1

The ID_AA64PFR0_EL1 characteristics are:

Purpose

Provides additional information about implemented processor features in AArch64.

The optional Advanced SIMD and floating-point support is not included in the base product of the processor. ARM requires licensees to have contractual rights to obtain the Advanced SIMD and floating-point support.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

ID_AA64PFR0_EL1 is architecturally mapped to external register EDPFR.

Attributes

ID_AA64PFR0_EL1 is a 64-bit register.

63	28	27	24	23	20	19	16	15	12	11	8	7	4	3	0
RES0		GIC		AdvSIMD		FP	EL3 handling		EL2 handling		EL1 handling		EL0 handling		

Figure B1-24 ID_AA64PFR0_EL1 bit assignments

[63:28]

Reserved, RES0.

GIC, [27:24]

GIC CPU interface:

0x0 GIC CPU interface is disabled, GICCDISABLE is HIGH, or not implemented.

0x1 GIC CPU interface is implemented and enabled, GICCDISABLE is low.

AdvSIMD, [23:20]

Advanced SIMD. The possible values are:

0x0 Advanced SIMD is implemented.

0xF Advanced SIMD is not implemented.

The FP and AdvSIMD both take the same value, as both must be implemented, or neither.

FP, [19:16]

Floating-point. The possible values are:

0x0 Floating-point is implemented.

0xF Floating-point is not implemented.

The FP and AdvSIMD both take the same value, as both must be implemented, or neither.

EL3 handling, [15:12]

EL3 exception handling:

0x1 Instructions can be executed at EL3.

EL2 handling, [11:8]

EL2 exception handling:

0x1 Instructions can be executed at EL2.

EL1 handling, [7:4]

EL1 exception handling. The possible values are:

0x1 Instructions can be executed at EL1.

EL0 handling, [3:0]

EL0 exception handling. The possible values are:

0x1 Instructions can be executed at EL0.

To access the ID_AA64PFR0_EL1:

```
MRS <Xt>, ID_AA64PFR0_EL1 ; Read ID_AA64PFR0_EL1 into Xt
```

Register access is encoded as follows:

Table B1-43 ID_AA64PFR0_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0100	000

The EDPFR can be accessed through the external debug interface, offset 0xD20.

B1.52 AArch64 Memory Model Feature Register 0, EL1

The ID_AA64MMFR0_EL1 characteristics are:

Purpose

Provides information about the implemented memory model and memory management support in the AArch64 Execution state.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

ID_AA64MMFR0_EL1 is a 64-bit register.

63	32	31	28	27	24	23	20	19	16	15	12	11	8	7	4	3	0
RES0		TGran4		TGran64		TGran16		BigEndELO		SNSMem		BigEnd		ASIDBits		PARange	

Figure B1-25 ID_AA64MMFR0_EL1 bit assignments

[63:32]

Reserved, RES0.

TGran4, [31:28]

Support for 4KB memory translation granule size:

0x0 Indicates that the 4KB granule is supported.

TGran64, [27:24]

Support for 64KB memory translation granule size:

0x0 Indicates that the 64KB granule is supported.

TGran16, [23:20]

Support for 16KB memory translation granule size:

0x1 Indicates that the 16KB granule is supported.

BigEndELO, [19:16]

Mixed-endian support only at EL0.

RES0

SNSMem, [15:12]

Secure versus Non-secure Memory distinction:

0b0001 Supports a distinction between Secure and Non-secure Memory.

BigEnd, [11:8]

Mixed-endian configuration support:

0b0001 Mixed-endian support. The SCTLR_ELx.EE and SCTLR_EL1.E0E bits are RW.

ASIDBits, [7:4]

Number of ASID bits:

0b0010 16 bits.

PARange, [3:0]

Physical address range supported:

0b0010 40 bits, 1TB.

To access the ID_AA64MMFR0_EL1:

```
MRS <Xt>, ID_AA64MMFR0_EL1 ; Read ID_AA64MMFR0_EL1 into Xt
```

Register access is encoded as follows:

Table B1-44 ID_AA64MMFR0_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0111	000

B1.53 Interrupt Status Register, EL1

The ISR_EL1 characteristics are:

Purpose

Shows whether an IRQ, FIQ, or external abort is pending. An indicated pending abort might be a physical abort or a virtual abort.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

ISR_EL1 is a 32-bit register.



Figure B1-26 ISR_EL1 bit assignments

[31:9]

Reserved, RES0.

A, [8]

External abort pending bit:

- 0 No pending external abort.
- 1 An external abort is pending.

I, [7]

IRQ pending bit. Indicates whether an IRQ interrupt is pending:

- 0 No pending IRQ.
- 1 An IRQ interrupt is pending.

F, [6]

FIQ pending bit. Indicates whether an FIQ interrupt is pending:

- 0 No pending FIQ.
- 1 An FIQ interrupt is pending.

[5:0]

Reserved, RES0.

To access the ISR_EL1:

```
MRS <Xt>, ISR_EL1 ; Read ISR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-45 ISR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	1100	0001	000

B1.54 L2 Auxiliary Control Register, EL1

The L2ACTLR_EL1 characteristics are:

Purpose

Provides configuration and control options for the L2 memory system.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

The L2ACTLR_EL1:

- This register can be written only when the L2 memory system is idle. ARM recommends that you write to this register after a powerup reset before the MMU is enabled and before any ACE, CHI or ACP traffic has begun. If the register must be modified after a powerup reset sequence, to idle the L2 memory system, you must take the following steps:
 1. Disable the MMU from each core followed by an ISB to ensure the MMU disable operation is complete, then followed by a DSB to drain previous memory transactions.
 2. Ensure that the system has no outstanding AC channel coherence requests to the Cortex-A34 processor.
 3. Ensure that the system has no outstanding ACP requests to the Cortex-A34 processor.

When the L2 memory system is idle, the processor can update the L2ACTLR_EL1 followed by an ISB. After the L2ACTLR_EL1 is updated, the MMUs can be enabled and normal ACE and ACP traffic can resume.

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

Attributes

L2ACTLR_EL1 is a 32-bit register.

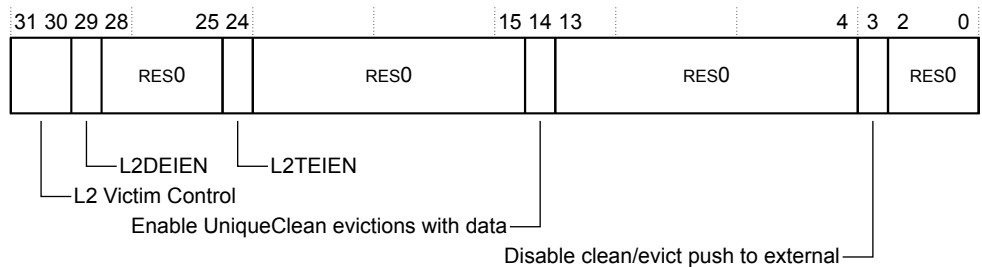


Figure B1-27 L2ACTLR_EL1 bit assignments

[31:30]

L2 Victim Control.

0b10 This is the default value. Software must not change it.

L2DEIEN, [29]

L2 cache data RAM error injection enable. The possible values are:

- 0 Normal behavior, errors are not injected. This is the reset value.
- 1 Double-bit errors are injected on all writes to the L2 cache data RAMs.

[28:25]

Reserved, RES0.

L2TEIEN, [24]

L2 cache tag RAM error injection enable. The possible values are:

- 0 Normal behavior, errors are not injected. This is the reset value.
- 1 Double-bit errors are injected on all writes to the L2 cache tag RAMs.

[23:15]

Reserved, RES0.

Enable UniqueClean evictions with data, [14]

Enables sending of WriteEvict transactions for UniqueClean evictions with data.

WriteEvict transactions update downstream caches that are outside the cluster. Enable WriteEvict transactions only if there is an L3 or system cache implemented in the system.

The possible values are:

- 0 Disables UniqueClean evictions with data. This is the reset value for ACE.
- 1 Enables UniqueClean evictions with data. This is the reset value for CHI.

In AXI implementations, this field is RES0.

Some ACE interconnects might not support the WriteEvict transaction. You must not enable this bit if your interconnect does not support WriteEvict transactions.

[13:4]

Reserved, RES0.

Disable clean/evict push to external, [3]

Disables sending of Evict transactions for clean cache lines that are evicted from the processor. This is required only if the external interconnect contains a snoop filter that requires notification when the processor evicts the cache line. The possible values are:

- 0 Enables clean/evict to be pushed out to external. This is the reset value for ACE.
- 1 Disables clean/evict from being pushed to external. This is the reset value for CHI.

In AXI implementations, this field is RES1.

[2:0]

Reserved, RES0.

To access the L2ACTLR_EL1:

```
MRS Rt, S3_1_C15_C0_0; Read L2ACTLR_EL1 into Rt
MSR S3_1_C15_C0_0, Rt; Write Rt to L2ACTLR_EL1
```

Register access is encoded as follows:

Table B1-46 L2ACTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0000	000

B1.55 L2 Control Register, EL1

The L2CTLR_EL1 characteristics are:

Purpose

Provides IMPLEMENTATION DEFINED control options for the L2 memory system.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
-	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

L2CTLR_EL1 is writable. However, all writes to this register are ignored.

Configurations

There are no configuration notes.

Attributes

L2CTLR_EL1 is a 32-bit register.

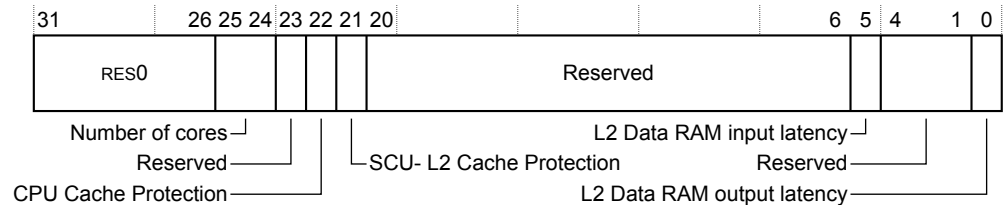


Figure B1-28 L2CTLR_EL1 bit assignments

[31:26]

Reserved, RES0.

Number of cores, [25:24]

Number of cores present:

- 0b00 One core, core 0.
- 0b01 Two cores, core 0 and core 1.
- 0b10 Three cores, cores 0 to 2.
- 0b11 Four cores, cores 0 to 3.

These bits are read-only and the value of this field is set to the number of cores present in the configuration.

[23]

Reserved, RES0.

CPU Cache Protection, [22]

CPU Cache Protection. Core RAMs are implemented:

- 0 Without ECC.
- 1 With ECC.

This field is RO.

SCU-L2 Cache Protection, [21]

SCU-L2 Cache Protection. L2 cache is implemented:

- 0 Without ECC.
- 1 With ECC.

This field is RO.

[20:6]

Reserved, RES0.

L2 data RAM input latency, [5]

L2 data RAM input latency:

0 1-cycle input delay from L2 data RAMs.

1 2-cycle input delay from L2 data RAMs.

This field is RO.

[4:1]

Reserved, RES0.

L2 data RAM output latency, [0]

L2 data RAM output latency:

0 2-cycle output delay from L2 data RAMs.

1 3-cycle output delay from L2 data RAMs.

This field is RO.

To access the L2CTLR_EL1:

```
MRS <Xt>, S3_1_C11_C0_2 ; Read L2CTLR_EL1 into Xt
MSR S3_1_C11_C0_2, <Xt>; Write Xt to L2CTLR_EL1
```

Register access is encoded as follows:

Table B1-47 L2CTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1011	0000	010

B1.56 L2 Extended Control Register, EL1

The L2ECTLR_EL1 characteristics are:

Purpose

Provides additional IMPLEMENTATION DEFINED control options for the L2 memory system. This register is used for dynamically changing, but implementation specific, control bits.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

The L2ECTLR_EL1 can be written dynamically.

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

There is one L2ECTLR_EL1 for the Cortex-A34 processor.

Attributes

L2ECTLR_EL1 is a 32-bit register.

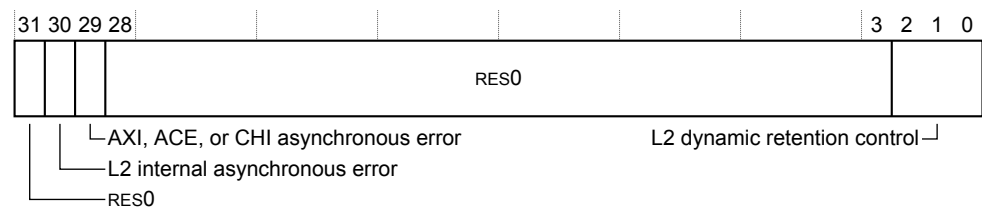


Figure B1-29 L2ECTLR_EL1 bit assignments

[31]

Reserved, RES0.

L2 internal asynchronous error, [30]

L2 internal asynchronous error caused by L2 RAM double-bit ECC error. The possible values are:

- 0 No pending asynchronous error. This is the reset value.
- 1 An asynchronous error has occurred.

A write of 0 clears this bit and drives **nINTERRIRQ** HIGH. A write of 1 is ignored.

AXI, ACE, or CHI asynchronous error, [29]

AXI, ACE, or CHI asynchronous error indication. The possible values are:

- 0 No pending asynchronous error.
- 1 An asynchronous error has occurred.

A write of 0 clears this bit and drives **nEXTERRIRQ** HIGH. A write of 1 is ignored.

[28:3]

Reserved, RES0.

L2 dynamic retention control, [2:0]

L2 dynamic retention control. The possible values are:

- 0b000 L2 dynamic retention disabled. This is the reset value.

- 0b001 2 Generic Timer ticks required before retention entry.
- 0b010 8 Generic Timer ticks required before retention entry.
- 0b011 32 Generic Timer ticks required before retention entry.
- 0b100 64 Generic Timer ticks required before retention entry.
- 0b101 128 Generic Timer ticks required before retention entry.
- 0b110 256 Generic Timer ticks required before retention entry.
- 0b111 512 Generic Timer ticks required before retention entry.

To access the L2ECTLR_EL1:

```
MRS Rt, S3_1_C11_C0_3; Read L2ECTLR_EL1 into Rt  
MSR S3_1_C11_C0_3, Rt; Write Rt to L2ECTLR_EL1
```

Register access is encoded as follows:

Table B1-48 L2ECTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1011	0000	011

B1.57 L2 Memory Error Syndrome Register, EL1

The L2MERRSR_EL1 characteristics are:

Purpose

Holds information about ECC errors on the:

- L2 data RAMs.
- L2 tag RAMs.
- SCU snoop filter RAMs.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

A write of any value to the register updates the register to $0x0000000000000000$.

Attributes

L2MERRSR_EL1 is a 64-bit register.

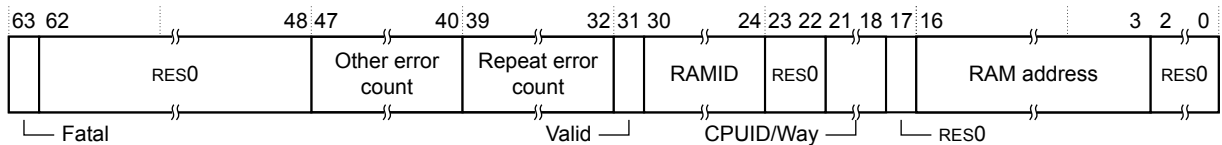


Figure B1-30 L2MERRSR_EL1 bit assignments

Fatal, [63]

Fatal bit. This bit is set to 1 on the first memory error that caused a data abort. It is a sticky bit so that after it is set, it remains set until the register is written.

The reset value is 0.

[62:48]

Reserved, RES0.

Other error count, [47:40]

This field is set to 0 on the first memory error and is incremented on any memory error that does not match the RAMID and Bank/Way information in this register while the sticky Valid bit is set.

The reset value is 0.

Repeat error count, [39:32]

This field is set to 0 on the first memory error and is incremented on any memory error that exactly matches the RAMID and Bank/Way information in this register while the sticky Valid bit is set.

The reset value is 0.

Valid, [31]

Valid bit. This bit is set to 1 on the first memory error. It is a sticky bit so that after it is set, it remains set until the register is written.

The reset value is 0.

RAMID, [30:24]

RAM Identifier. Indicates the RAM in which the first memory error occurred. The possible values are:

- 0x10 L2 tag RAM.
- 0x11 L2 data RAM.
- 0x12 SCU snoop filter RAM.

[23:22]

Reserved, RES0.

CPUID/Way, [21:18]

Indicates the RAM where the first memory error occurred.

L2 tag RAM

- 0x0 Way 0
- 0x1 Way 1
- ...
- 0x6 Way 6
- 0x7 Way 7

L2 data RAM

- 0x0 Bank 0
- 0x1 Bank 1
- ...
- 0x7 Bank 7
- 0x8-0xF Unused

SCU snoop filter RAM

- 0x0 CPU0:Way0
- 0x1 CPU0:Way1
- ...
- 0xE CPU3:Way2
- 0xF CPU3:Way3

[17]

Reserved, RES0.

RAM address, [16:3]

Indicates the index address of the first memory error.

[2:0]

Reserved, RES0.

- A fatal error results in the RAMID, CPU ID/Way and RAM address recording the fatal error, even if the sticky bit was set.
- If two or more memory errors in the same RAM occur in the same cycle, only one error is reported.
- If two or more first memory error events from different RAMs occur in the same cycle, one of the errors is selected arbitrarily, while the Other error count field is incremented only by one.
- If two or more memory error events from different RAMs, that do not match the RAMID, bank, way, or index information in this register while the sticky Valid bit is set, occur in the same cycle, the Other error count field is incremented only by one.

To access the L2MERRSR_EL1:

```
MRS <Xt>, S3_1_C15_C2_3 ; Read L2MERRSR_EL1 into Xt
MSR S3_1_C15_C2_3, <Xt> ; Write Xt into L2MERRSR_EL1
```

Register access is encoded as follows:

Table B1-49 L2MERRSR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	001	1111	0010	011

B1.58 Memory Attribute Indirection Register, EL1

The MAIR_EL1 characteristics are:

Purpose

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.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

MAIR_EL1 is permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

MAIR_EL1 is a 64-bit register.

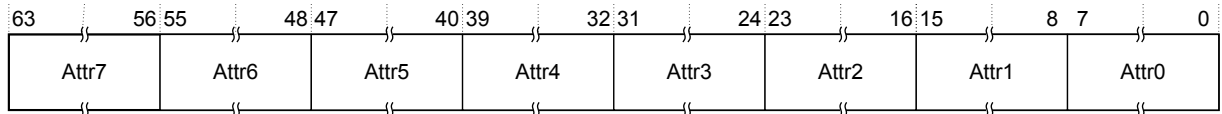


Figure B1-31 MAIR_EL1 bit assignments

Attr<n> is the memory attribute encoding for an AttrIdx[2:0] entry in a Long descriptor format translation table entry, where AttrIdx[2:0] gives the value of <n> in Attr<n>.

Table B1-50 Attr<n>[7:4] bit assignments

Bits	Meaning
0b0000	Device memory. See Table B1-51 Attr<n>[3:0] bit assignments on page B1-231
0b00RW, RW not 00	Normal Memory, Outer Write-through transient. The transient hint is ignored.
0b0100	Normal Memory, Outer Non-Cacheable.
0b01RW, RW not 00	Normal Memory, Outer Write-back transient. The transient hint is ignored.
0b10RW	Normal Memory, Outer Write-through non-transient.
0b11RW	Normal Memory, Outer Write-back non-transient.

Table B1-51 Attr<n>[3:0] bit assignments

Bits	Meaning when Attr<n>[7:4] is 0000	Meaning when Attr<n>[7:4] is not 0000
0b0000	Device-nGnRnE memory	UNPREDICTABLE
0b00RW, RW not 00	UNPREDICTABLE	Normal Memory, Inner Write-through transient
0b0100	Device-nGnRE memory	Normal memory, Inner Non-Cacheable
0b01RW, RW not 00	UNPREDICTABLE	Normal Memory, Inner Write-back transient
0b1000	Device-nGRE memory	Normal Memory, Inner Write-through non-transient (RW=00)
0b10RW, RW not 00	UNPREDICTABLE	Normal Memory, Inner Write-through non-transient

Table B1-51 Attr<n>[3:0] bit assignments (continued)

Bits	Meaning when Attr<n>[7:4] is 0000	Meaning when Attr<n>[7:4] is not 0000
0b1100	Device-GRE memory	Normal Memory, Inner Write-back non-transient (RW=00)
0b11RW, RW not 00	UNPREDICTABLE	Normal Memory, Inner Write-back non-transient

The following table shows the encoding of the R and W bits that are used, in some Attr<n> encodings in [Table B1-51 Attr<n>\[3:0\] bit assignments on page B1-231](#) and [Table B1-50 Attr<n>\[7:4\] bit assignments on page B1-231](#), to define the read-allocate and write-allocate policies:

Table B1-52 Encoding of R and W bits in some Attrm fields

R or W	Meaning
0	Do not allocate
1	Allocate

To access the MAIR_EL1:

```
MRS <Xt>, MAIR_EL1 ; Read EL1 Memory Attribute Indirection Register
MSR MAIR_EL1, <Xt> ; Write EL1 Memory Attribute Indirection Register
```

Register access is encoded as follows:

Table B1-53 MAIR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	1010	0010	000

B1.59 Memory Attribute Indirection Register, EL2

The MAIR_EL2 characteristics are:

Purpose

Provides the memory attribute encodings corresponding to the possible AttrIndx values in a Long-descriptor format translation table entry for stage 1 translations at EL2.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

MAIR_EL2 is permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

MAIR_EL2 is a 64-bit register.

The MAIR_EL2 bit assignments follow the same pattern as described in [B1.58 Memory Attribute Indirection Register, EL1](#) on page B1-231.

To access the MAIR_EL2:

```
MRS <Xt>, MAIR_EL2 ; Read EL2 Memory Attribute Indirection Register
MSR MAIR_EL2, <Xt> ; Write EL2 Memory Attribute Indirection Register
```

Register access is encoded as follows:

Table B1-54 MAIR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	1010	0010	000

B1.60 Memory Attribute Indirection Register, EL3

The MAIR_EL3 characteristics are:

Purpose

Provides the memory attribute encodings corresponding to the possible AttrIndx values in a Long-descriptor format translation table entry for stage 1 translations at EL3.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

MAIR_EL2 is permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

MAIR_EL3 is a 64-bit register.

The MAIR_EL3 bit assignments follow the same pattern as described in [B1.58 Memory Attribute Indirection Register, EL1](#) on page B1-231.

To access the MAIR_EL3:

```
MRS <Xt>, MAIR_EL3 ; Read EL3 Memory Attribute Indirection Register
MSR MAIR_EL3, <Xt> ; Write EL3 Memory Attribute Indirection Register
```

Register access is encoded as follows:

Table B1-55 MAIR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	1010	0010	000

B1.61 Monitor Debug Configuration Register, EL2

The MDCR_EL2 characteristics are:

Purpose

Provides EL2 configuration options for self-hosted debug and the Performance Monitors extension.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
(S)	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

- If EL2 is not implemented, this register is RES0 from EL3.

Attributes

MDCR_EL2 is a 32-bit register.

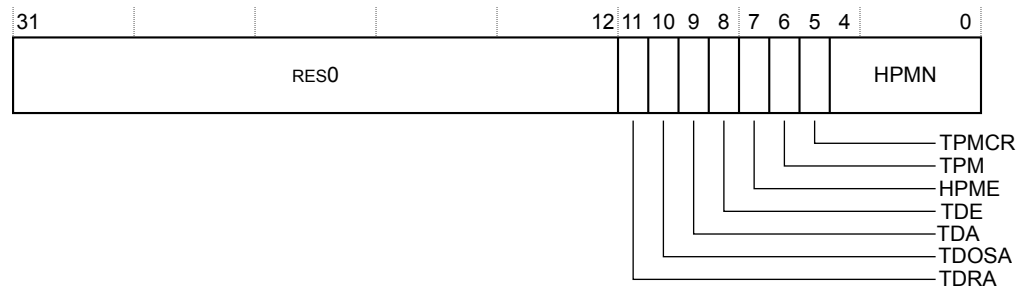


Figure B1-32 MDCR_EL2 bit assignments

[31:12]

Reserved, RES0.

TDRA, [11]

Trap debug ROM address register access.

- 0 Has no effect on accesses to debug ROM address registers from EL1 and EL0.
- 1 Trap valid Non-secure EL1 and EL0 access to debug ROM address registers to Hyp mode.

When this bit is set to 1, any access to MDRAR_EL1 from EL1 or EL0 is trapped to EL2.

If HCR_EL2.TGE is 1 or MDCR_EL2.TDE is 1, then this bit is ignored and treated as though it is 1 other than for the value read back from MDCR_EL2.

On Warm reset, the field resets to 0.

TDOSA, [10]

Trap Debug OS-related register access:

- 0 Has no effect on accesses to OS-related debug registers.
- 1 Trap valid Non-secure accesses to OS-related debug registers to EL2.

When this bit is set to 1, any access to OSLAR_EL1, OSLSR_EL1, OSDLR_EL1, DBGPRCR_EL1 from EL0 or EL1 is trapped to EL2.

If HCR_EL2.TGE is 1 or MDCR_EL2.TDE is 1, then this bit is ignored and treated as though it is 1 other than for the value read back from MDCR_EL2.

On Warm reset, the field resets to 0.

TDA, [9]

Trap Debug Access:

- 0 Has no effect on accesses to Debug registers.
- 1 Trap valid Non-secure accesses to Debug registers to EL2.

When this bit is set to 1, any valid Non-secure access to the debug registers from EL1 or EL0, other than the registers trapped by the TDRA and TDOSA bits, is trapped to EL2.

If HCR_EL2.TGE is 1 or MDCR_EL2.TDE is 1, then this bit is ignored and treated as though it is 1 other than for the value read back from MDCR_EL2.

On Warm reset, the field resets to 0.

TDE, [8]

Trap software debug exceptions:

- 0 Has no effect on software debug exceptions.
- 1 Route Software debug exceptions from Non-secure EL1 and EL0 to EL2. Also enables traps on all debug register accesses to EL2.

If HCR_EL2.TGE is 1, then this bit is ignored and treated as though it is 1 other than for the value read back from MDCR_EL2. This bit resets to 0.

HPME, [7]

Hypervisor Performance Monitor Enable:

- 0 EL2 performance monitor counters disabled.
- 1 EL2 performance monitor counters enabled.

When this bit is set to 1, the Performance Monitors counters that are reserved for use from EL2 or Secure state are enabled. For more information see the description of the HPMN field.

The reset value of this bit is UNKNOWN.

TPM, [6]

Trap Performance Monitor accesses:

- 0 Has no effect on performance monitor accesses.
- 1 Trap Non-secure EL0 and EL1 accesses to Performance Monitors registers that are not UNALLOCATED to EL2.

This bit resets to 0.

TPMCR, [5]

Trap PMCR_EL0 accesses:

- 0 Has no effect on PMCR_EL0 accesses.
- 1 Trap Non-secure EL0 and EL1 accesses to PMCR_EL0 to EL2.

This bit resets to 0.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

HPMN, [4:0]

Hyp Performance Monitor count. Defines the number of Performance Monitors counters that are accessible from Non-secure EL1 and EL0 modes.

In Non-secure state, HPMN divides the Performance Monitors counters as follows. For counter n in Non-secure state:

For example, If PMnEVCNTR is performance monitor counter n then, in Non-secure state:

- If n is in the range $0 \leq n < \text{HPMN}$, the counter is accessible from EL1 and EL2, and from EL0 if permitted by PMUSERENR_EL0. PMCR_EL0.E enables the operation of counters in this range.
- There are six performance counters, specified by PMCR.N.

If n is in the range $\text{HPMN} \leq n < 6$, the counter is accessible only from EL2. MDCR_EL2.HPME enables the operation of counters in this range.

If the field is set to 0, then Non-secure EL0 or EL1 has no access to any counters.

If the field is set to a value greater than six, the behavior is the same as if the value is six.

For reads of MDCR_EL2.HPMN by EL2 or higher, if this field is set to 0 or to a value larger than PMCR_EL0.N, the processor returns the value that was written to MDCR_EL2.HPMN.

This field resets to 0x6.

To access the MDCR_EL2:

```
MRS <Xt>, MDCR_EL2 ; Read MDCR_EL2 into Xt
MSR MDCR_EL2, <Xt> ; Write Xt to MDCR_EL2
```

Register access is encoded as follows:

Table B1-56 MDCR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0001	0001	001

B1.62 Monitor Debug Configuration Register, EL3

The MDCR_EL3 characteristics are:

Purpose

Provides configuration options for Security to self-hosted debug.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

MDCR_EL3 is a 32-bit register.

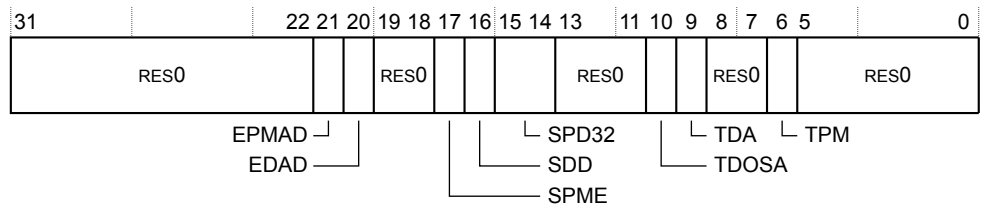


Figure B1-33 MDCR_EL3 bit assignments

[31:22]

Reserved, RES0.

EPMA, [21]

External debugger access to Performance Monitors registers disabled. This disables access to these registers by an external debugger. The possible values are:

- 0 Access to Performance Monitors registers from external debugger is permitted.
- 1 Access to Performance Monitors registers from external debugger is disabled, unless overridden by authentication interface.

EDAD, [20]

External debugger access to breakpoint and watchpoint registers disabled. This disables access to these registers by an external debugger. The possible values are:

- 0 Access to breakpoint and watchpoint registers from external debugger is permitted.
- 1 Access to breakpoint and watchpoint registers from external debugger is disabled, unless overridden by authentication interface.

[19:18]

Reserved, RES0.

SPME, [17]

Secure performance monitors enable. This enables event counting exceptions from Secure state. The possible values are:

- 0 Event counting prohibited in Secure state. This is the reset value.
- 1 Event counting allowed in Secure state.

SDD, [16]

AArch64 secure debug disable. Disables Software debug exceptions from Secure state if Secure EL1 is using AArch64, other than from Software breakpoint instructions. The possible values are:

- 0 Debug exceptions from Secure EL0 are enabled, and debug exceptions from Secure EL1 are enabled if MDSCR_EL1.KDE is 1 and PSTATE.D is 0.
- 1 Debug exceptions from all exception levels in Secure state are disabled.

The reset value is UNKNOWN.

SPD32, [15:14]

Reserved, RES0.

[13:11]

Reserved, RES0.

TDOSA, [10]

Trap accesses to the OS debug system registers, OSLAR_EL1, OSLSR_EL1, OSDLR_EL1, and DBGPRCR_EL1 OS.

- 0 Accesses are not trapped.
- 1 Accesses to the OS debug system registers are trapped to EL3.

The reset value is UNKNOWN.

TDA, [9]

Trap accesses to the remaining sets of debug registers to EL3.

- 0 Accesses are not trapped.
- 1 Accesses to the remaining debug system registers are trapped to EL3.

The reset value is UNKNOWN.

[8:7]

Reserved, RES0.

TPM, [6]

Trap Performance Monitors accesses. The possible values are:

- 0 Accesses are not trapped.
- 1 Accesses to the Performance Monitor registers are trapped to EL3.

The reset value is UNKNOWN.

[5:0]

Reserved, RES0.

To access the MDCR_EL3:

MRS <Xt>, MDCR_EL3 ; Read EL3 Monitor Debug Configuration Register
 MSR MDCR_EL3, <Xt> ; Write EL3 Monitor Debug Configuration Register

Register access is encoded as follows:

Table B1-57 MDCR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0001	0011	001

B1.63 Monitor Debug System Control Register, EL1

The MDSCR_EL1 characteristics are:

Purpose

Main control register for the debug implementation.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

MDSCR_EL1 is a 32-bit register.

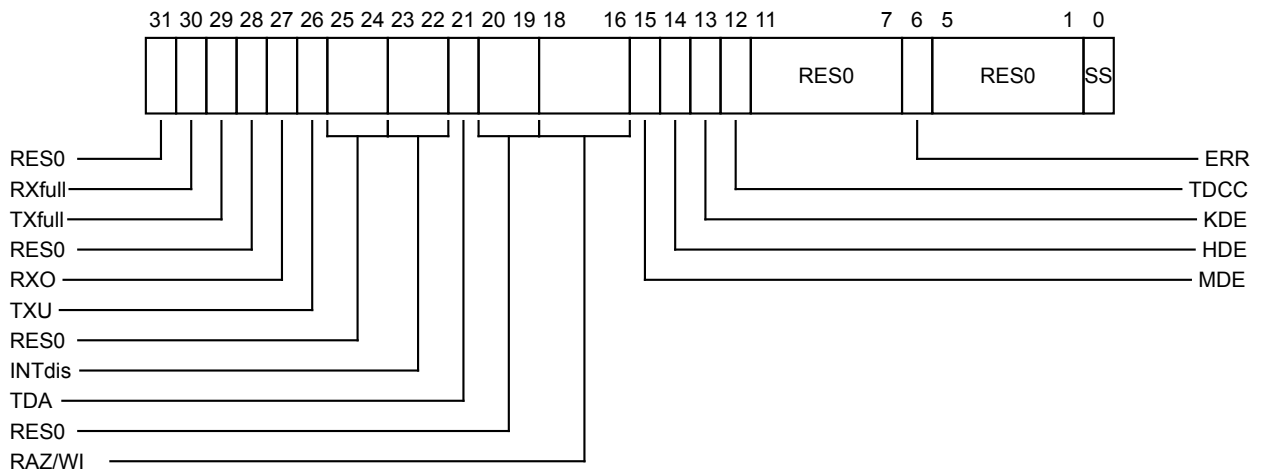


Figure B1-34 MDSCR_EL1 bit assignments

[31]

Reserved, RES0.

RXfull, [30]

Used for save/restore of EDSCR.RXfull

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO, and software must treat it as UNK/SBZP.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

TXfull, [29]

Used for save/restore of EDSCR.RXfull

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO, and software must treat it as UNK/SBZP.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

[28]

Reserved, RES0.

RXO, [27]

Used for save/restore of EDSCR.RXO.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

TXU, [26]

Used for save/restore of EDSCR.TXU.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

[25:24]

Reserved, RES0.

INTdis, [23:22]

Used for save/restore of EDSCR.INTdis.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

TDA, [21]

Used for save/restore of EDSCR.TDA.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

[20:19]

Reserved, RES0.

[18:16]

Reserved, RAZ/WI. Hardware must implement this as RAZ/WI. Software must not rely on this property as the behavior of reserved values might change in a future revision of the architecture.

MDE, [15]

Reserved, RES0.

HDE, [14]

Used for save/restore of EDSCR.HDE.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

KDE, [13]

Local (kernel) debug enable. If EL_D is using AArch64, enable Software debug events within EL_D. Permitted values are:

- 0** Software debug events, other than Software breakpoint instructions, disabled within EL_D.
- 1** Software debug events enabled within EL_D.

When this register has an architecturally-defined reset value, this field resets to a value that is architecturally UNKNOWN on Warm reset.

TDCC, [12]

Traps EL0 accesses to the DCC registers to EL1, from both Execution states:

- 0** EL0 using AArch64:
 - EL0 accesses to the MDCCSR_EL0, DBGDTR_EL0, DBGDTRTX_EL0, and DBGDTRRX_EL0 registers are not trapped to EL1.

1 EL0 using AArch64:

- EL0 accesses to the MDCCSR_EL0, DBGDTR_EL0, DBGDTRTX_EL0, and DBGDTRRX_EL0 registers are trapped to EL1.

When this register has an architecturally-defined reset value, this field resets to a value that is architecturally UNKNOWN on Warm reset.

[11:7]

Reserved, RES0.

ERR, [6]

Used for save/restore of EDSCR.ERR.

- When OSLSR_EL1.OSLK == 0 (the OS lock is unlocked), this bit is RO. Software must treat it as UNKNOWN and use an SBZP policy for writes.
- When OSLSR_EL1.OSLK == 1 (the OS lock is locked), this bit is RW.

[5:1]

Reserved, RES0.

SS, [0]

Software step control bit. If EL_D is using AArch64, enable Software step. Permitted values are:

- 0** Software step is disabled.
- 1** Software step is enabled.

When this register has an architecturally-defined reset value, this field resets to a value that is architecturally UNKNOWN on Warm reset.

To access the MDSCR_EL1:

```
MRS <Xt>, MDSCR_EL1 ; Read MDSCR_EL1 into Xt
MSR MDSCR_EL1, <Xt> ; Write Xt to MDSCR_EL1
```

Register access is encoded as follows:

Table B1-58 MDSCR_EL1 access encoding

op0	op1	CRn	CRm	op2
10	000	0000	0010	010

B1.64 Main ID Register, EL1

The MIDR_EL1 characteristics are:

Purpose

Provides identification information for the processor, including an implementer code for the device and a device ID number.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

The MIDR_EL1 is architecturally mapped to external MIDR_EL1 register.

Attributes

MIDR_EL1 is a 32-bit register.

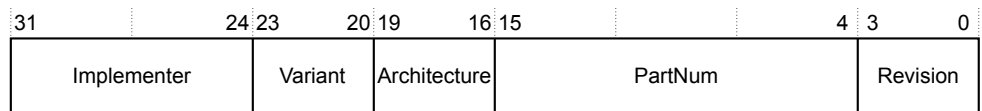


Figure B1-35 MIDR_EL1 bit assignments

Implementer, [31:24]

Indicates the implementer code. This value is:

0x41 ASCII character 'A' - implementer is ARM.

Variant, [23:20]

Indicates the variant number of the processor. This is the major revision number *x* in the *rx* part of the *rxpy* description of the product revision status. This value is:

0x0 r0p1.

Architecture, [19:16]

Indicates the architecture code. This value is:

0xF Defined by CPUID scheme.

PartNum, [15:4]

Indicates the primary part number. This value is:

0xD02 Cortex-A34 processor.

Revision, [3:0]

Indicates the minor revision number of the processor. This is the minor revision number *y* in the *py* part of the *rxpy* description of the product revision status. This value is:

0x1 r0p1.

To access the MIDR_EL1:

```
MRS <Xt>, MIDR_EL1 ; Read MIDR_EL1 into Xt
```

Table B1-59 MIDR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0000	000

The MIDR_EL1 can be accessed through the external debug interface, offset 0xD00.

B1.65 Multiprocessor Affinity Register, EL1

The MPIDR_EL1 characteristics are:

Purpose

Provides an additional core identification mechanism for scheduling purposes in a cluster system.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
-	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

MPIDR_EL1[31:0] is:

- Mapped to external register EDDEVAF0.

MPIDR_EL1[63:32] is:

- Mapped to external register EDDEVAF1.

Attributes

MPIDR_EL1 is a 64-bit register.

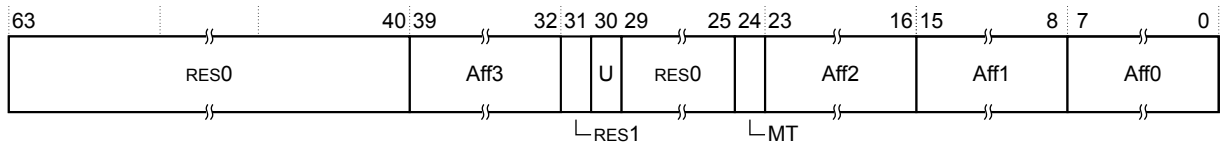


Figure B1-36 MPIDR_EL1 bit assignments

[63:40]

Reserved, RES0.

Aff3, [39:32]

Affinity level 3. Highest level affinity field.

Reserved, RES0.

[31]

Reserved, RES1.

U, [30]

Indicates a single core system, as distinct from core 0 in a cluster. This value is:

- 0 Processor is part of a multiprocessor system. This is the value for implementations with more than one core, and for implementations with an ACE or CHI master interface.
- 1 Processor is part of a uniprocessor system. This is the value for single core implementations with an AXI master interface.

[29:25]

Reserved, RES0.

MT, [24]

Indicates whether the lowest level of affinity consists of logical cores that are implemented using a multi-threading type approach. This value is:

- 0 Performance of cores at the lowest affinity level is largely independent.

Aff2, [23:16]

Affinity level 2. Second highest level affinity field.

Indicates the value read in the **CLUSTERIDAFF2** configuration signal.

Aff1, [15:8]

Affinity level 1. Third highest level affinity field.

Indicates the value read in the **CLUSTERIDAFF1** configuration signal.

Aff0, [7:0]

Affinity level 0. Lowest level affinity field.

Indicates the core number in the Cortex-A34 processor. The possible values are:

- 0x0 A cluster with one core only.
- 0x0, 0x1 A cluster with two cores.
- 0x0, 0x1, 0x2 A cluster with three cores.
- 0x0, 0x1, 0x2, 0x3 A cluster with four cores.

To access the MPIDR_EL1:

```
MRS <Xt>, MPIDR_EL1 ; Read MPIDR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-60 MPIDR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0000	101

The EDDEVAFF0 and EDDEVAFF1 can be accessed through the external debug interface, offsets 0xFA8 and 0xFAC respectively.

B1.66 Physical Address Register, EL1

The PAR_EL1 characteristics are:

Purpose

The Physical Address returned from an address translation.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

PAR_EL1 is a 64-bit register.

The following figure shows the PAR_EL1 bit assignments when the Virtual Address to Physical Address conversion completes successfully.

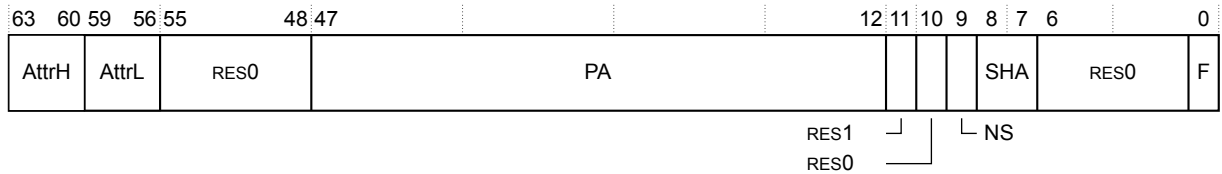


Figure B1-37 PAR_EL1 pass bit assignments

The following list shows the PAR_EL1 bit assignments when the Virtual Address to Physical Address conversion completes successfully.

AttrH, [63:60]

Defines Normal or Device memory and outer cacheability. Must be used in conjunction with AttrL. The possible values are:

- 0b0000 Device memory, see Attr[3:0].
- 0b0100 Normal memory, Outer Non-cacheable.
- 0b1000 Normal memory, Outer Write-Through Cacheable.
- 0b1001 Normal memory, Outer Write-Through Cacheable, Outer Write-Allocate.
- 0b1010 Normal memory, Outer Write-Through Cacheable, Outer Read-Allocate.
- 0b1011 Normal memory, Outer Write-Through Cacheable, Outer WriteAllocate, Outer Read-Allocate.
- 0b1100 Normal memory, Outer Write-Back Cacheable.
- 0b1101 Normal memory, Outer Write-Back Cacheable, Outer Write-Allocate.
- 0b1110 Normal memory, Outer Write-Back Cacheable, Outer Read-Allocate.
- 0b1111 Normal memory, Outer Write-Back Cacheable, Outer Write-Allocate, Outer Read-Allocate.

All other values are reserved.

AttrL, [59:56]

Defines Device memory, and Inner cacheability. Must be interpreted in conjunction with AttrH. The possible values are:

- 0b0000 Device (nGnRnE) memory if AttrH is 0b0000. Otherwise this value is reserved.

- 0b0100 Device (not nGnRnE) memory if AttrH is 0b0000. Otherwise, Normal memory, Inner Non-cacheable.
- 0b1000 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Through Cacheable.
- 0b1001 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Through Cacheable, Inner Write-Allocate.
- 0b1010 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Through Cacheable, Inner Read-Allocate.
- 0b1011 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Through Cacheable, Inner Write-Allocate, Inner Read-Allocate.
- 0b1100 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Back Cacheable.
- 0b1101 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Back Cacheable, Inner Write-Allocate.
- 0b1110 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Back Cacheable, Inner Read-Allocate.
- 0b1111 Reserved if AttrH is 0b0000. Otherwise, Normal memory, Inner Write-Through Cacheable, Inner Write-Allocate, Inner Read-Allocate.

All other values are reserved.

[55:48]

Reserved, RES0.

PA, [47:12]

Physical address. The Physical Address corresponding to the supplied Virtual Address. Returns address bits[47:12].

[11]

Reserved, RES1.

[10]

Reserved, RES0.

NS, [9]

Non-secure. The NS attribute for a translation table entry read from Secure state.

This bit is UNKNOWN for a translation table entry from Non-secure state.

SHA, [8:7]

Shareability attribute for the Physical Address returned from a translation table entry. The possible values are:

- 0b00 Non-shareable.
- 0b01 Reserved.
- 0b10 Outer Shareable
- 0b11 Inner Shareable.

Takes the value of 0b10 for:

- Any type of device memory.
- Normal memory with both Inner Non-cacheable and Outer-cacheable attributes.

[6:1]

Reserved, RES0.

F, [0]

Pass/Fail bit. Indicates whether the conversion completed successfully. This value is:

- 0 Virtual Address to Physical Address conversion completed successfully.

The following figure shows the PAR_EL1 bit assignments when the Virtual Address to Physical Address conversion is aborted.

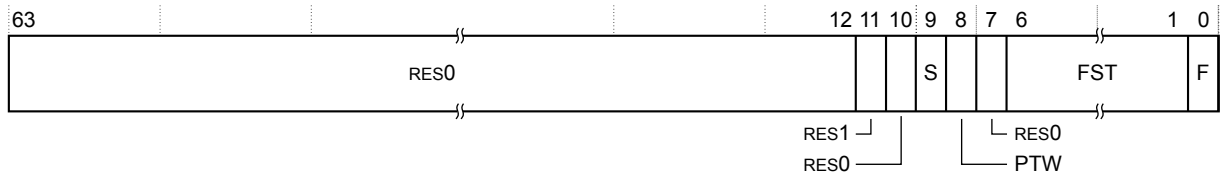


Figure B1-38 PAR_EL1 fail bit assignments

The following list shows the PAR_EL1 bit assignments when the Virtual Address to Physical Address conversion is aborted.

[63:12]

Reserved, RES0.

[11]

Reserved, RES1.

[10]

Reserved, RES0.

S, [9]

Stage of fault. Indicates the state where the translation aborted. The possible values are:

- 0 Translation aborted because of a fault in stage 1 translation.
- 1 Translation aborted because of a fault in stage 2 translation.

PTW, [8]

Indicates a stage 2 fault during a stage 1 table walk. The possible values are:

- 0 No stage 2 fault during a stage 1 table walk.
- 1 Translation aborted because of a stage 2 fault during a stage 1 table walk.

[7]

Reserved, RES0.

FST, [6:1]

Fault status code, as the Data Abort ESR encoding shows it. See the *ARM Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

F, [0]

Pass/Fail bit. Indicates whether the conversion completed successfully. This value is:

- 1 Virtual Address to Physical Address conversion aborted.

To access the PAR_EL1:

```
MRS <Xt>, PAR_EL1 ; Read EL1 Physical Address Register
MSR PAR_EL1, <Xt> ; Write EL1 Physical Address Register
```

Register access is encoded as follows:

Table B1-61 PAR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0111	0100	000

B1.67 Revision ID Register, EL1

The REVIDR_EL1 characteristics are:

Purpose

Provides implementation-specific minor revision information that can be interpreted only in conjunction with the Main ID Register.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RO	RO	RO	RO	RO

Configurations

There are no configuration notes.

Attributes

REVIDR_EL1 is a 32-bit register.

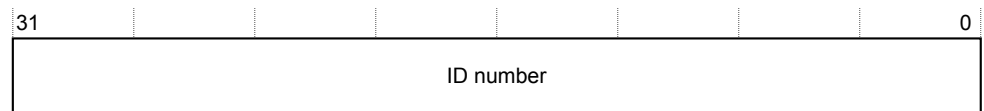


Figure B1-39 REVIDR_EL1 bit assignments

ID number, [31:0]

Implementation-specific revision information. The reset value is determined by the specific Cortex-A34 processor implementation.

0x00000000

Revision code is zero.

To access the REVIDR_EL1:

```
MRS <Xt>, REVIDR_EL1 ; Read REVIDR_EL1 into Xt
```

Register access is encoded as follows:

Table B1-62 REVIDR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0000	0000	110

B1.68 Reset Management Register, EL3

The RMR_EL3 characteristics are:

Purpose

Controls the execution state that the processor boots into and allows request of a warm reset.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

RMR_EL3 is a 32-bit register.

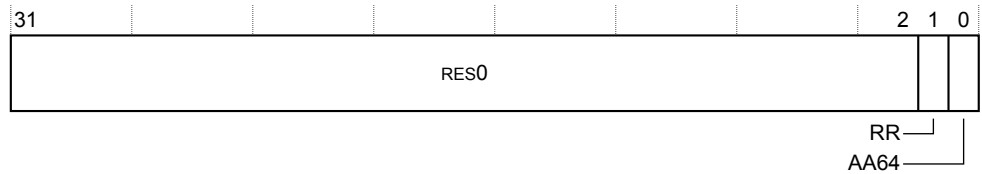


Figure B1-40 RMR_EL3 bit assignments

[31:2]

Reserved, RES0.

RR, [1]

Reset Request. The possible values are:

- 0 This is the reset value.
- 1 Requests a warm reset. This bit is set to 0 by either a cold or warm reset.

The bit is strictly a request.

AA64, [0]

Reserved. RES1

To access the RMR_EL3:

```
MRS <Xt>, RMR_EL3 ; Read RMR_EL3 into Xt
MSR RMR_EL3, <Xt> ; Write Xt to RMR_EL3
```

Register access is encoded as follows:

Table B1-63 RMR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	1100	0000	010

B1.69 Reset Vector Base Address Register, EL3

The RVBAR_EL3 characteristics are:

Purpose

Contains the address that execution starts from after reset when executing in the AArch64 state.

RVBAR_EL3 is part of the Reset management registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RO	RO

Configurations

There is no configuration information.

Attributes

RVBAR_EL3 is a 64-bit register.

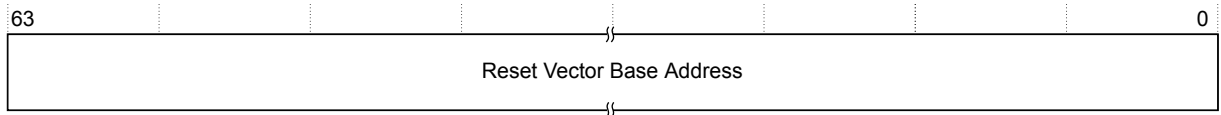


Figure B1-41 RVBAR_EL3 bit assignments

RVBA, [63:0]

Reset Vector Base Address. The address that execution starts from after reset when executing in 64-bit state. Bits[1:0] of this register are 0b00, as this address must be aligned, and bits [63:40] are 0x000000 because the address must be within the physical address size supported by the processor.

To access the RVBAR_EL3:

```
MRS <Xt>, RVBAR_EL3 ; Read RVBAR_EL3 into Xt
```

Register access is encoded as follows:

Table B1-64 RVBAR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	1100	0000	001

B1.70 Secure Configuration Register, EL3

The SCR_EL3 characteristics are:

Purpose

Defines the configuration of the security state. SCR_EL3 specifies:

- Security state of EL0 and EL1, either Secure or Non-secure.
- Register width at lower exception levels.
- The exception level that the processor takes exceptions at, if an IRQ, FIQ, or external abort occurs.

SCR_EL3 is part of the Security registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

SCR_EL3 is a 32-bit register.

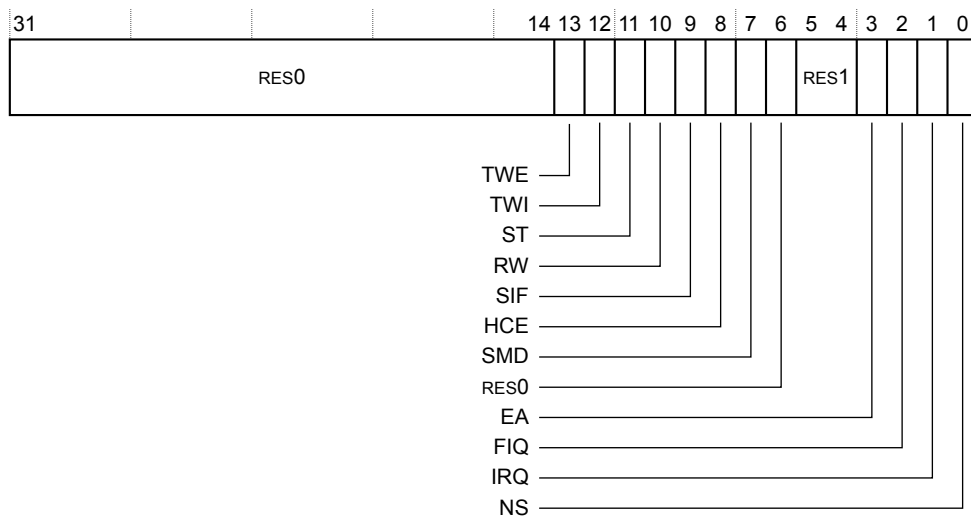


Figure B1-42 SCR_EL3 bit assignments

[31:14]

Reserved, RES0.

TWE, [13]

Traps WFE instructions. The possible values are:

- 0 WFE instructions are not trapped. This is the reset value.
- 1 WFE instructions executed from EL2, EL1, or EL0 are trapped to EL3 if the instruction would otherwise cause suspension of execution, that is if:
 - The event register is not set.
 - There is not a pending WFE wakeup event.
 - The instruction is not trapped at EL2 or EL1.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

TWI, [12]

Traps WFI instructions. The possible values are:

- 0 WFI instructions are not trapped. This is the reset value.
- 1 WFI instructions executed from EL2, EL1, or EL0 are trapped to EL3 if the instruction would otherwise cause suspension of execution, that is if there is not a pending WFI wakeup event and the instruction is not trapped at EL2 or EL1.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

ST, [11]

Enable Secure EL1 access to CNTPS_TVAL_EL1, CNTS_CTL_EL1, and CNTPS_CVAL_EL1 registers. The possible values are:

- 0 Registers accessible only in EL3. This is the reset value.
- 1 Registers accessible in EL3 and EL1 when SCR_EL3.NS is 0.

RW, [10]

RAO/WI.

SIF, [9]

Secure Instruction Fetch. When the processor is in Secure state, this bit disables instruction fetches from Non-secure memory. The possible values are:

- 0 Secure state instruction fetches from Non-secure memory are permitted. This is the reset value.
- 1 Secure state instruction fetches from Non-secure memory are not permitted.

HCE, [8]

Hyp Call enable. This bit enables the use of HVC instructions. The possible values are:

- 0 The HVC instruction is UNDEFINED at all exception levels. This is the reset value.
- 1 The HVC instruction is enabled at EL1, EL2 or EL3.

SMD, [7]

SMC instruction disable. The possible values are:

- 0 The SMC instruction is enabled at EL1, EL2, and EL3. This is the reset value.
- 1 The SMC instruction is UNDEFINED at all exception levels. At EL1, in the Non-secure state, the HCR_EL2.TSC bit has priority over this control.

[6]

Reserved, RES0.

[5:4]

Reserved, RES1.

EA, [3]

External Abort and SError interrupt Routing. This bit controls which mode takes external aborts. The possible values are:

- 0 External Aborts and SError Interrupts while executing at exception levels other than EL3 are not taken in EL3. This is the reset value.
- 1 External Aborts and SError Interrupts while executing at all exception levels are taken in EL3.

FIQ, [2]

Physical FIQ Routing. The possible values are:

- 0 Physical FIQ while executing at exception levels other than EL3 are not taken in EL3. This is the reset value.
- 1 Physical FIQ while executing at all exception levels are taken in EL3.

IRQ, [1]

Physical IRQ Routing. The possible values are:

- 0 Physical IRQ while executing at exception levels other than EL3 are not taken in EL3.
- 1 Physical IRQ while executing at all exception levels are taken in EL3.

NS, [0]

Non-secure bit. The possible values are. The possible values are:

- 0 EL0 and EL1 are in Secure state, memory accesses from those exception levels can access Secure memory. This is the reset value.
- 1 EL0 and EL1 are in Non-secure state, memory accesses from those exception levels cannot access Secure memory.

To access the SCR_EL3:

```
MRS <Xt>, SCR_EL3 ; Read SCR_EL3 into Xt
MSR SCR_EL3, <Xt> ; Write Xt to SCR_EL3
```

Register access is encoded as follows:

Table B1-65 SCR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0001	0001	000

B1.71 System Control Register, EL1

The SCTL_R_EL1 characteristics are:

Purpose

Provides top level control of the system, including its memory system at EL1.

SCTL_R_EL1 is part of the Virtual memory control registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

SCTL_R_EL1 is a 32-bit register.

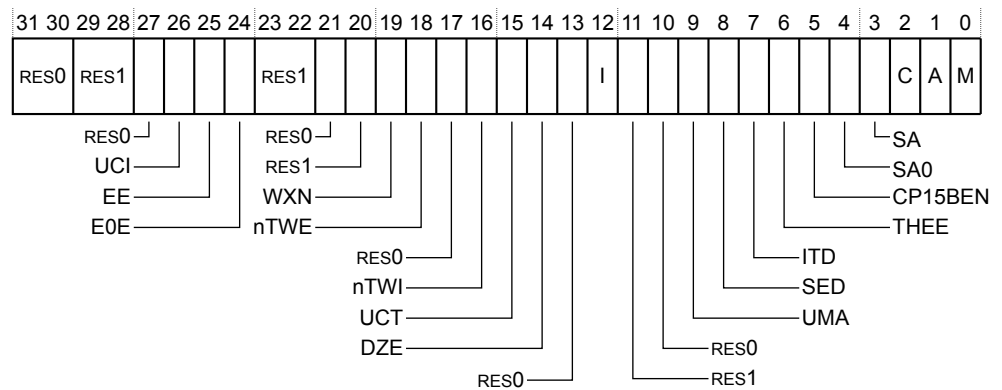


Figure B1-43 SCTL_R_EL1 bit assignments

[31:30]

Reserved, RES0.

[29:28]

Reserved, RES1.

[27]

Reserved, RES0.

UCI, [26]

Enables EL0 access to the DC CVAU, DC CIVAC, DC CVAC and IC IVAU instructions in the AArch64 Execution state. The possible values are:

- 0 EL0 access disabled. This is the reset value.
- 1 EL0 access enabled.

EE, [25]

Exception endianness. The value of this bit controls the endianness for explicit data accesses at EL1. This value also indicates the endianness of the translation table data for translation table lookups. The possible values of this bit are:

- 0 Little-endian.
- 1 Big-endian.

The reset value of this bit is determined by the CFGEND configuration pin.

E0E, [24]

Endianness of explicit data access at EL0. The possible values are:

- 0 Explicit data accesses at EL0 are little-endian. This is reset value.
- 1 Explicit data accesses at EL0 are big-endian.

[23:22]

Reserved, RES1.

[21]

Reserved, RES0.

[20]

Reserved, RES1.

WXN, [19]

Write permission implies *Execute Never* (XN). This bit can be used to require all memory regions with write permissions to be treated as XN. The possible values are:

- 0 Regions with write permission are not forced XN. This is the reset value.
- 1 Regions with write permissions are forced XN.

nTWE, [18]

WFE non-trapping. The possible values are:

- 0 A WFE instruction executed at EL0, that, if this bit was set to 1, would permit entry to a low-power state, is trapped to EL1.
- 1 WFE instructions executed as normal. This is the reset value.

[17]

Reserved, RES0.

nTWI, [16]

WFI non-trapping. The possible values are:

- 0 A WFI instruction executed at EL0, that, if this bit was set to 1, would permit entry to a low-power state, is trapped to EL1.
- 1 WFI instructions executed as normal. This is the reset value.

UCT, [15]

Enables EL0 access to the CTR_EL0 register in AArch64 Execution state. The possible values are:

- 0 Disables EL0 access to the CTR_EL0 register. This is the reset value.
- 1 Enables EL0 access to the CTR_EL0 register.

DZE, [14]

Enables access to the DC ZVA instruction at EL0. The possible values are:

- 0 Disables execution access to the DC ZVA instruction at EL0. The instruction is trapped to EL1. This is the reset value.
- 1 Enables execution access to the DC ZVA instruction at EL0.

[13]

Reserved, RES0.

I, [12]

Instruction cache enable. The possible values are:

- 0 Instruction caches disabled. This is the reset value.
- 1 Instruction caches enabled.

[11]

Reserved, RES1.

[10]

Reserved, RES0.

UMA, [9]

User Mask Access. Controls access to interrupt masks from EL0, when EL0 is using AArch64.

The possible values of this bit are:

- 0 Disable access to the interrupt masks from EL0.
- 1 Enable access to the interrupt masks from EL0.

SED, [8]

Reserved. RES1.

ITD, [7]

Reserved. RES1.

THEE, [6]

RES0 T32EE is not implemented.

CP15BEN, [5]

Reserved. RES0.

SA0, [4]

Enable EL0 stack alignment check. The possible values are:

- 0 Disable EL0 stack alignment check.
- 1 Enable EL0 stack alignment check. This is the reset value.

SA, [3]

Enable SP alignment check. The possible values are:

- 0 Disable SP alignment check.
- 1 Enable SP alignment check. This is the reset value.

C, [2]

Cache enable. The possible values are:

- 0 Data and unified caches disabled. This is the reset value.
- 1 Data and unified caches enabled.

A, [1]

Alignment check enable. The possible values are:

- 0 Alignment fault checking disabled. This is the reset value.
- 1 Alignment fault checking enabled.

M, [0]

MMU enable. The possible values are:

- 0 EL1 and EL0 stage 1 MMU disabled. This is the reset value.
- 1 EL1 and EL0 stage 1 MMU enabled.

To access the SCTLR_EL1:

```
MRS <Xt>, SCTLR_EL1 ; Read SCTLR_EL1 into Xt
MSR SCTLR_EL1, <Xt> ; Write Xt to SCTLR_EL1
```

Register access is encoded as follows:

Table B1-66 SCTLR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0001	0000	000

B1.72 System Control Register, EL2

The SCTL_R_EL2 characteristics are:

Purpose

Provides top level control of the system, including its memory system at EL2.

SCTL_R_EL2 is part of:

- The Virtual memory control registers functional group.
- The Hypervisor and virtualization registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

SCTL_R_EL2 is a 32-bit register.

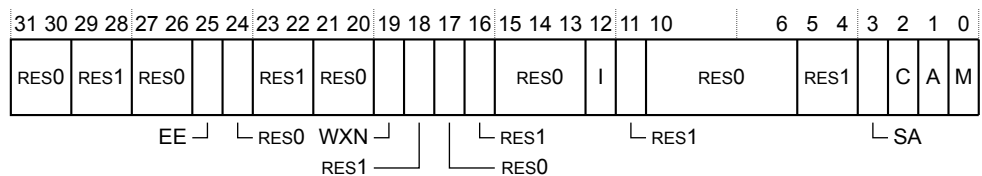


Figure B1-44 SCTL_R_EL2 bit assignments

[31:30]

Reserved, RES0.

[29:28]

Reserved, RES1.

[27:26]

Reserved, RES0.

EE, [25]

Exception endianness. The possible values are:

- 0 Little endian.
- 1 Big endian.

The reset value depends on the value of the CFGEND configuration input.

[24]

Reserved, RES0.

[23:22]

Reserved, RES1.

[21:20]

Reserved, RES0.

WXN, [19]

Force treatment of all memory regions with write permissions as XN. The possible values are:

- 0 Regions with write permissions are not forced XN. This is the reset value.
- 1 Regions with write permissions are forced XN.

[18]

Reserved, RES1.

- [17]** Reserved, RES0.
- [16]** Reserved, RES1.
- [15:13]** Reserved, RES0.
- I, [12]** Instruction cache enable. The possible values are:
 0 Instruction caches disabled. This is the reset value.
 1 Instruction caches enabled.
- [11]** Reserved, RES1.
- [10:6]** Reserved, RES0.
- [5:4]** Reserved, RES1.
- SA, [3]** Enables stack alignment check. The possible values are:
 0 Disables stack alignment check.
 1 Enables stack alignment check. This is the reset value.
- C, [2]** Global enable for data and unifies caches. The possible values are:
 0 Disables data and unified caches. This is the reset value.
 1 Enables data and unified caches.
- A, [1]** Enable alignment fault check The possible values are:
 0 Disables alignment fault checking. This is the reset value.
 1 Enables alignment fault checking.
- M, [0]** Global enable for the EL2 MMU. The possible values are:
 0 Disables EL2 MMU. This is the reset value.
 1 Enables EL2 MMU.

To access the SCTLR_EL2:

```
MRS <Xt>, SCTLR_EL2 ; Read SCTLR_EL2 into Xt
MSR SCTLR_EL2, <Xt> ; Write Xt to SCTLR_EL2
```

Register access is encoded as follows:

Table B1-67 SCTLR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0001	0000	000

B1.73 System Control Register, EL3

The SCTLR_EL3 characteristics are:

Purpose

Provides top level control of the system, including its memory system at EL3.

SCTLR_EL3 is part of the Virtual memory control registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

SCTLR_EL3 is a 32-bit register.

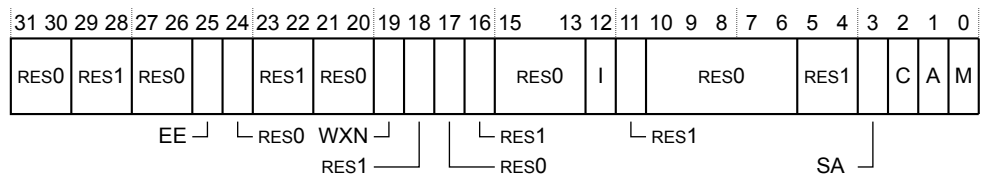


Figure B1-45 SCTLR_EL3 bit assignments

[31:30]

Reserved, RES0.

[29:28]

Reserved, RES1.

[27:26]

Reserved, RES0.

EE, [25]

Exception endianness. This bit controls the endianness for:

- Explicit data accesses at EL3.
- Stage 1 translation table walks at EL3.

The possible values are:

- 0 Little endian. This is the reset value.
- 1 Big endian.

[24]

Reserved, RES0.

[23:22]

Reserved, RES1.

[21:20]

Reserved, RES0.

WXN, [19]

Force treatment of all memory regions with write permissions as XN. The possible values are:

- 0 Regions with write permissions are not forced XN. This is the reset value.
- 1 Regions with write permissions are forced XN.

- [18]** Reserved, RES1.
- [17]** Reserved, RES0.
- [16]** Reserved, RES1.
- [15:13]** Reserved, RES0.
- I, [12]** Global instruction cache enable. The possible values are:
 - 0 Instruction caches disabled. This is the reset value.
 - 1 Instruction caches enabled.
- [11]** Reserved, RES1.
- [10:6]** Reserved, RES0.
- [5:4]** Reserved, RES1.
- SA, [3]** Enables stack alignment check. The possible values are:
 - 0 Disables stack alignment check.
 - 1 Enables stack alignment check. This is the reset value.
- C, [2]** Global enable for data and unifies caches. The possible values are:
 - 0 Disables data and unified caches. This is the reset value.
 - 1 Enables data and unified caches.
- A, [1]** Enable alignment fault check The possible values are:
 - 0 Disables alignment fault checking. This is the reset value.
 - 1 Enables alignment fault checking.
- M, [0]** Global enable for the EL3 MMU. The possible values are:
 - 0 Disables EL3 MMU. This is the reset value.
 - 1 Enables EL3 MMU.

To access the SCTLR_EL3:

```
MRS <Xt>, SCTLR_EL3 ; Read SCTLR_EL3 into Xt
MSR SCTLR_EL3, <Xt> ; Write Xt to SCTLR_EL3
```

Register access is encoded as follows:

Table B1-68 SCTLR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0001	0000	000

B1.74 Translation Control Register, EL1

The TCR_EL1 characteristics are:

Purpose

Determines which Translation Base Registers defines the base address register for a translation table walk required for stage 1 translation of a memory access from EL0 or EL1 and holds cacheability and shareability information.

TCR_EL1 is part of the Virtual memory control registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
-	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

TCR_EL1 is a 64-bit register.

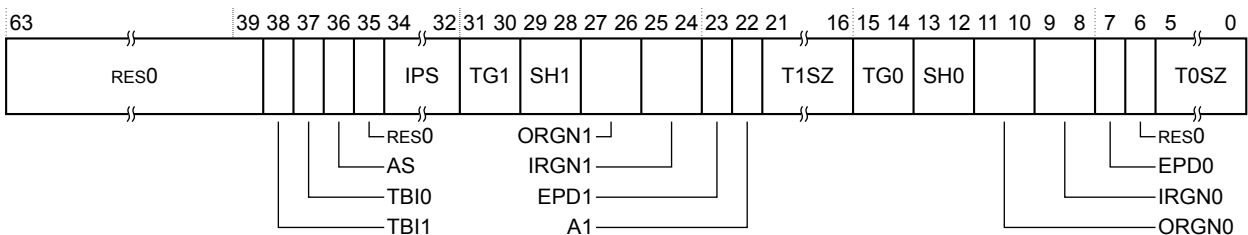


Figure B1-46 TCR_EL1 bit assignments

[63:39]

Reserved, RES0.

TBI1, [38]

Top Byte Ignored. Indicates whether the top byte of the input address is used for address match for the TTBR1_EL1 region. The possible values are:

- 0 Top byte used in the address calculation.
- 1 Top byte ignored in the address calculation.

TBI0, [37]

Top Byte Ignored. Indicates whether the top byte of the input address is used for address match for the TTBR0_EL1 region. The possible values are:

- 0 Top byte used in the address calculation.
- 1 Top byte ignored in the address calculation.

AS, [36]

ASID size. The possible values are:

- 0 8-bit.
- 1 16-bit.

[35]

Reserved, RES0.

IPS, [34:32]

Intermediate Physical Address Size. The possible values are:

- 0b000 32 bits, 4GB.
- 0b001 36 bits, 64GB.
- 0b010 40 bits, 1TB.

All other values are reserved.

TG1, [31:30]

TTBR1_EL1 granule size. The possible values are:

- 0b00 Reserved.
- 0b10 4KB.
- 0b01 16KB.
- 0b11 64KB.

All other values are not supported.

SH1, [29:28]

Shareability attribute for memory associated with translation table walks using TTBR1_EL1. The possible values are:

- 0b00 Non-shareable.
- 0b01 Reserved.
- 0b10 Outer shareable.
- 0b11 Inner shareable.

ORGN1, [27:26]

Outer cacheability attribute for memory associated with translation table walks using TTBR1_EL1. The possible values are:

- 0b00 Normal memory, Outer Non-cacheable.
- 0b01 Normal memory, Outer Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Outer Write-Through Cacheable.
- 0b11 Normal memory, Outer Write-Back no Write-Allocate Cacheable.

IRGN1, [25:24]

Inner cacheability attribute for memory associated with translation table walks using TTBR1_EL1. The possible values are:

- 0b00 Normal memory, Inner Non-cacheable.
- 0b01 Normal memory, Inner Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Inner Write-Through Cacheable.
- 0b11 Normal memory, Inner Write-Back no Write-Allocate Cacheable.

EPD1, [23]

Translation table walk disable for translations using TTBR1_EL1. Controls whether a translation table walk is performed on a TLB miss for an address that is translated using TTBR1_EL1. The possible values are:

- 0 Perform translation table walk using TTBR1_EL1.
- 1 A TLB miss on an address translated from TTBR1_EL1 generates a Translation fault. No translation table walk is performed.

A1, [22]

Selects whether TTBR0_EL1 or TTBR1_EL1 defines the ASID. The possible values are:

- 0 TTBR0_EL1.ASID defines the ASID.
- 1 TTBR1_EL1.ASID defines the ASID.

T1SZ, [21:16]

Size offset of the memory region addressed by TTBR1_EL1. The region size is $2^{(64-T1SZ)}$ bytes.

TG0, [15:14]

TTBR0_EL1 granule size. The possible values are:

- 0b00 4KB.
- 0b10 16KB.
- 0b01 64KB.
- 0b11 Reserved.

All other values are not supported.

SH0, [13:12]

Shareability attribute for memory associated with translation table walks using TTBR0_EL1.

The possible values are:

- 0b00 Non-shareable.
- 0b01 Reserved.
- 0b10 Outer shareable.
- 0b11 Inner shareable.

ORGN0, [11:10]

Outer cacheability attribute for memory associated with translation table walks using TTBR0_EL1. The possible values are:

- 0b00 Normal memory, Outer Non-cacheable.
- 0b01 Normal memory, Outer Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Outer Write-Through Cacheable.
- 0b11 Normal memory, Outer Write-Back no Write-Allocate Cacheable.

IRGN0, [9:8]

Inner cacheability attribute for memory associated with translation table walks using TTBR0_EL1. The possible values are:

- 0b00 Normal memory, Inner Non-cacheable.
- 0b01 Normal memory, Inner Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Inner Write-Through Cacheable.
- 0b11 Normal memory, Inner Write-Back no Write-Allocate Cacheable.

EPD0, [7]

Translation table walk disable for translations using TTBR0_EL1. Controls whether a translation table walk is performed on a TLB miss for an address that is translated using TTBR0_EL1. The possible values are:

- 0 Perform translation table walk using TTBR0_EL1.
- 1 A TLB miss on an address translated from TTBR0_EL1 generates a Translation fault. No translation table walk is performed.

[6]

Reserved, RES0.

T0SZ, [5:0]

Size offset of the memory region addressed by TTBR0_EL1. The region size is $2^{(64-T0SZ)}$ bytes.

To access the TCR_EL1:

```
MRS <Xt>, TCR_EL1 ; Read TCR_EL1 into Xt
MSR TCR_EL1, <Xt> ; Write Xt to TCR_EL1
```

Register access is encoded as follows:

Table B1-69 TCR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0010	0000	010

B1.75 Translation Control Register, EL2

The TCR_EL2 characteristics are:

Purpose

Controls translation table walks required for stage 1 translation of a memory access from EL2 and holds cacheability and shareability information.

TCR_EL2 is part of:

- The Virtual memory control registers functional group.
- The Hypervisor and virtualization registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

TCR_EL2 is a 32-bit register.

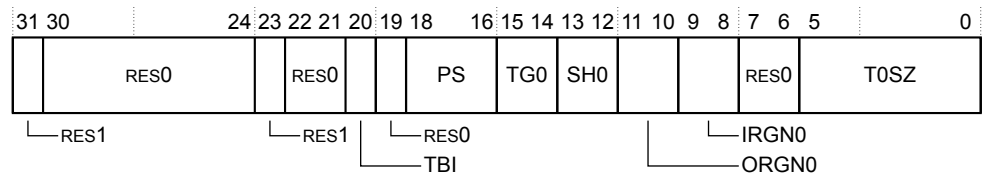


Figure B1-47 TCR_EL2 bit assignments

[31]

Reserved, RES1.

[30:24]

Reserved, RES0.

[23]

Reserved, RES1.

[22:21]

Reserved, RES0.

TBI, [20]

Top Byte Ignored. Indicates whether the top byte of the input address is used for address match. The possible values are:

- 0 Top byte used in the address calculation.
- 1 Top byte ignored in the address calculation.

[19]

Reserved, RES0.

PS, [18:16]

Physical address size. The possible values are:

- 0b000 32 bits, 4GB.
- 0b001 36 bits, 64GB.
- 0b010 40 bits, 1TB.

Other values are reserved.

TG0, [15:14]

TTBR0_EL2 granule size. The possible values are:

- 0b00 4KB.
- 0b10 16KB.
- 0b01 64KB.
- 0b11 Reserved.

All other values are not supported.

SH0, [13:12]

Shareability attribute for memory associated with translation table walks using TTBR0_EL2.

The possible values are:

- 0b00 Non-shareable.
- 0b01 Reserved.
- 0b10 Outer shareable.
- 0b11 Inner shareable.

ORGN0, [11:10]

Outer cacheability attribute for memory associated with translation table walks using TTBR0_EL2. The possible values are:

- 0b00 Normal memory, Outer Non-cacheable.
- 0b01 Normal memory, Outer Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Outer Write-Through Cacheable.
- 0b11 Normal memory, Outer Write-Back no Write-Allocate Cacheable.

IRGN0, [9:8]

Inner cacheability attribute for memory associated with translation table walks using TTBR0_EL2. The possible values are:

- 0b00 Normal memory, Inner Non-cacheable.
- 0b01 Normal memory, Inner Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Inner Write-Through Cacheable.
- 0b11 Normal memory, Inner Write-Back no Write-Allocate Cacheable.

[7:6]

Reserved, RES0.

T0SZ, [5:0]

Size offset of the memory region addressed by TTBR0_EL2. The region size is $2^{(64-T0SZ)}$ bytes.

To access the TCR_EL2:

```
MRS <Xt>, TCR_EL2 ; Read EL2 Translation Control Register
MSR TCR_EL2, <Xt> ; Write EL2 Translation Control Register
```

Register access is encoded as follows:

Table B1-70 TCR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0010	0000	010

B1.76 Translation Control Register, EL3

The TCR_EL3 characteristics are:

Purpose

Controls translation table walks required for stage 1 translation of memory accesses from EL3 and holds cacheability and shareability information for the accesses.

TCR_EL3 is part of the Virtual memory control registers functional group.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

TCR_EL3 is a 32-bit register.

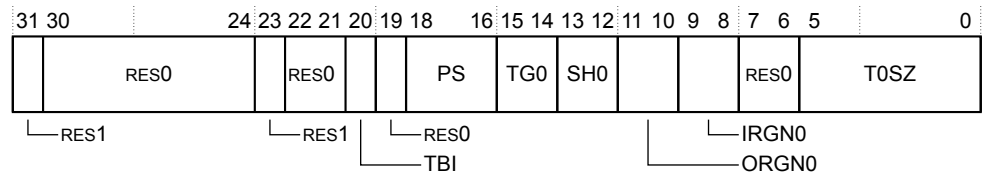


Figure B1-48 TCR_EL3 bit assignments

[31]

Reserved, RES1.

[30:24]

Reserved, RES0.

[23]

Reserved, RES1.

[22:21]

Reserved, RES0.

TBI, [20]

Top Byte Ignored. Indicates whether the top byte of the input address is used for address match.

The possible values are:

- 0 Top byte used in the address calculation.
- 1 Top byte ignored in the address calculation.

[19]

Reserved, RES0.

PS, [18:16]

Physical address size. The possible values are:

- 0b000 32 bits, 4GB.
- 0b001 36 bits, 64GB.
- 0b010 40 bits, 1TB.

Other values are reserved.

TG0, [15:14]

TTBR0_EL3 granule size. The possible values are:

- 0b00 4KB.
- 0b10 16KB.
- 0b01 64KB.
- 0b11 Reserved.

All other values are not supported.

SH0, [13:12]

Shareability attribute for memory associated with translation table walks using TTBR0_EL3.

The possible values are:

- 0b00 Non-shareable.
- 0b01 Reserved.
- 0b10 Outer shareable.
- 0b11 Inner shareable.

ORGN0, [11:10]

Outer cacheability attribute for memory associated with translation table walks using TTBR0_EL3.

The possible values are:

- 0b00 Normal memory, Outer Non-cacheable.
- 0b01 Normal memory, Outer Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Outer Write-Through Cacheable.
- 0b11 Normal memory, Outer Write-Back no Write-Allocate Cacheable.

IRGN0, [9:8]

Inner cacheability attribute for memory associated with translation table walks using TTBR0_EL3.

The possible values are:

- 0b00 Normal memory, Inner Non-cacheable.
- 0b01 Normal memory, Inner Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Inner Write-Through Cacheable.
- 0b11 Normal memory, Inner Write-Back no Write-Allocate Cacheable.

[7:6]

Reserved, RES0.

T0SZ, [5:0]

Size offset of the memory region addressed by TTBR0_EL3. The region size is $2^{(64-T0SZ)}$ bytes.

To access the TCR_EL3:

```
MRS <Xt>, TCR_EL3 ; Read EL3 Translation Control Register
MRS TCR_EL3, <Xt> ; Read EL3 Translation Control Register
```

Register access is encoded as follows:

Table B1-71 TCR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0010	0000	010

B1.77 Translation Table Base Register 0, EL1

The TTBR0_EL1 characteristics are:

Purpose

Holds the base address of translation table 0, and information about the memory it occupies. This is one of the translation tables for the stage 1 translation of memory accesses from modes other than Hyp mode.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Any of the fields in this register are permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

TTBR0_EL1 is 64-bit register.



Figure B1-49 TTBR0_EL1 bit assignments

ASID, [63:48]

An ASID for the translation table base address. The TCR_EL1.A1 field selects either TTBR0_EL1.ASID or TTBR1_EL1.ASID.

BADDR[47:x], [47:0]

Translation table base address, bits[47:x]. Bits [x-1:0] are RES0.

x is based on the value of TCR_EL1.T0SZ, the stage of translation, and the memory translation granule size.

For instructions on how to calculate it, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*

The value of x determines the required alignment of the translation table, that must be aligned to 2^x bytes.

If bits [x-1:0] are not all zero, this is a misaligned Translation Table Base Address. Its effects are CONSTRAINED UNPREDICTABLE, where bits [x-1:0] are treated as if all the bits are zero. The value read back from those bits is the value written.

To access the TTBR0_EL1:

```
MRS <Xt>, TTBR0_EL1 ; Read TTBR0_EL1 into Xt
MSR TTBR0_EL1, <Xt> ; Write Xt to TTBR0_EL1
```

Register access is encoded as follows:

Table B1-72 TTBR0_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0010	0000	000

B1.78 Translation Table Base Register 0, EL3

The TTBR0_EL3 characteristics are:

Purpose

Holds the base address of the translation table for the stage 1 translation of memory accesses from EL3.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

TTBR0_EL3 is a 64-bit register.

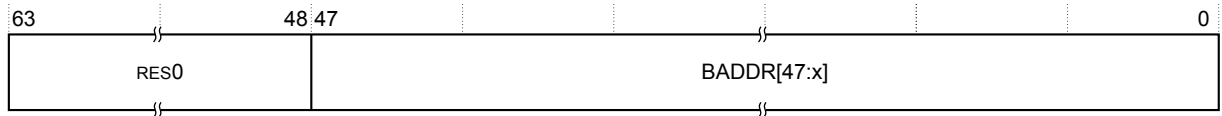


Figure B1-50 TTBR0_EL3 bit assignments

[63:48]

Reserved, RES0.

BADDR[47:x], [47:0]

Translation table base address, bits[47:x]. Bits [x-1:0] are RES0.

x is based on the value of TCR_EL1.T0SZ, the stage of translation, and the memory translation granule size.

For instructions on how to calculate it, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

The value of x determines the required alignment of the translation table, that must be aligned to 2^x bytes.

If bits [x-1:0] are not all zero, this is a misaligned Translation Table Base Address. Its effects are CONstrained UNPREDICTABLE, where bits [x-1:0] are treated as if all the bits are zero. The value read back from those bits is the value written.

To access the TTBR0_EL3:

```
MRS <Xt>, TTBR0_EL3 ; Read TTBR0_EL3 into Xt
MSR TTBR0_EL3, <Xt> ; Write Xt to TTBR0_EL3
```

Register access is encoded as follows:

Table B1-73 TTBR0_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	0010	0000	000

B1.79 Translation Table Base Register 1, EL1

The TTBR1_EL1 characteristics are:

Purpose

Holds the base address of translation table 1, and information about the memory it occupies. This is one of the translation tables for the stage 1 translation of memory accesses at EL0 and EL1.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Any of the fields in this register are permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

TTBR1_EL1 is a 64-bit register.

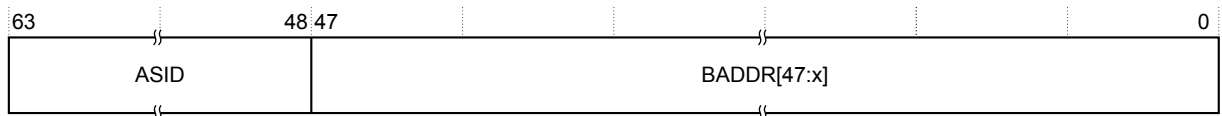


Figure B1-51 TTBR1_EL1 bit assignments

ASID, [63:48]

An ASID for the translation table base address. The TCR_EL1.A1 field selects either TTBR0_EL1.ASID or TTBR1_EL1.ASID.

BADDR[47:x], [47:0]

Translation table base address, bits[47:x]. Bits [x-1:0] are RES0.

x is based on the value of TCR_EL1.T0SZ, the stage of translation, and the memory translation granule size.

For instructions on how to calculate it, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

The value of x determines the required alignment of the translation table, that must be aligned to 2^x bytes.

If bits [x-1:0] are not all zero, this is a misaligned Translation Table Base Address. Its effects are CONSTRAINED UNPREDICTABLE, where bits [x-1:0] are treated as if all the bits are zero. The value read back from those bits is the value written.

To access the TTBR1_EL1:

```
MRS <Xt>, TTBR1_EL1 ; Read TTBR1_EL1 into Xt
MSR TTBR1_EL1, <Xt> ; Write Xt to TTBR1_EL1
```

Register access is encoded as follows:

Table B1-74 TTBR1_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	0010	0000	001

B1.80 Vector Base Address Register, EL1

The VBAR_EL1 characteristics are:

Purpose

Holds the exception base address for any exception that is taken to EL1.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

VBAR_EL1 is a 64-bit register.

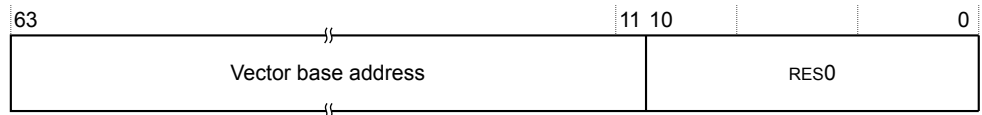


Figure B1-52 VBAR_EL1 bit assignments

Vector base address, [63:11]

Base address of the exception vectors for exceptions taken in this exception level.

[10:0]

Reserved, RES0.

To access the VBAR_EL1:

```
MRS <Xt>, VBAR_EL1 ; Read VBAR_EL1 into Xt
MSR VBAR_EL1, <Xt> ; Write Xt to VBAR_EL1
```

Register access is encoded as follows:

Table B1-75 VBAR_EL1 access encoding

op0	op1	CRn	CRm	op2
11	000	1100	0000	000

B1.81 Vector Base Address Register, EL2

The VBAR_EL2 characteristics are:

Purpose

Holds the exception base address for any exception that is taken to EL2.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Configurations

There are no configuration notes.

Attributes

VBAR_EL2 is a 64-bit register.

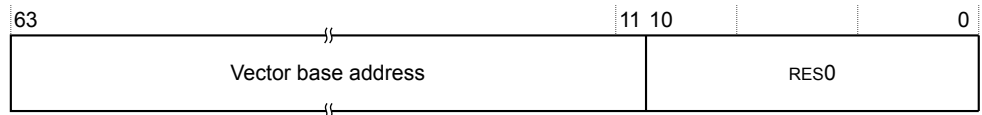


Figure B1-53 VBAR_EL2 bit assignments

Vector base address, [63:11]

Base address of the exception vectors for exceptions taken in this exception level.

[10:0]

Reserved, RES0.

To access the VBAR_EL2:

```
MRS <Xt>, VBAR_EL2 ; Read VBAR_EL2 into Xt
MSR VBAR_EL2, <Xt> ; Write Xt to VBAR_EL2
```

Register access is encoded as follows:

Table B1-76 VBAR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	1100	0000	000

B1.82 Vector Base Address Register, EL3

The VBAR_EL3 characteristics are:

Purpose

Holds the exception base address for any exception that is taken to EL3.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	-	RW	RW

Configurations

There are no configuration notes.

Attributes

VBAR_EL3 is a 64-bit register.

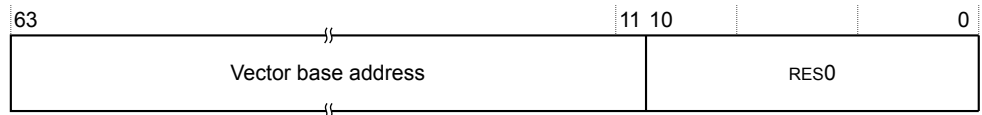


Figure B1-54 VBAR_EL3 bit assignments

Vector base address, [63:11]

Base address of the exception vectors for exceptions taken in this exception level.

[10:0]

Reserved, RES0.

To access the VBAR_EL3:

MRS <Xt>, VBAR_EL3 ; Read EL3 Vector Base Address Register
 MSR VBAR_EL3, <Xt> ; Write EL3 Vector Base Address Register

Register access is encoded as follows:

Table B1-77 VBAR_EL3 access encoding

op0	op1	CRn	CRm	op2
11	110	1100	0000	000

B1.83 Virtualization Multiprocessor ID Register, EL2

The VMPIDR_EL2 characteristics are:

Purpose

Provides the value of the Virtualization Multiprocessor ID. This is the value returned by Non-secure EL1 reads of MPIDR.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	-

Configurations

There are no configuration notes.

Attributes

VMPIDR_EL2 is a 64-bit register.

VMPIDR_EL2 resets to the value of MPIDR_EL2.

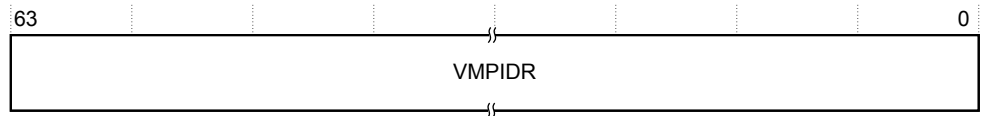


Figure B1-55 VMPIDR_EL2 bit assignments

VMPIDR, [63:0]

MPIDR value returned by Non-secure EL1 reads of the MPIDR_EL1. The MPIDR description defines the subdivision of this value. See [Figure B1-36 MPIDR_EL1 bit assignments on page B1-245](#).

To access the VMPIDR_EL2:

MRS <Xt>, VMPIDR_EL2 ; Read VMPIDR_EL2 into Xt
 MSR VMPIDR_EL2, <Xt> ; Write Xt to VMPIDR_EL2

Register access is encoded as follows:

Table B1-78 VMPIDR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0000	0000	101

B1.84 Virtualization Processor ID Register, EL2

The VPIDR_EL2 characteristics are:

Purpose

Holds the value of the Virtualization Processor ID. This is the value returned by Non-secure EL1 reads of MIDR_EL1. See [Figure B1-35 MIDR_EL1 bit assignments on page B1-243](#).

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	-

Configurations

There are no configuration notes.

Attributes

VPIDR_EL2 is a 32-bit register.

VPIDR_EL2 resets to the value of MIDR_EL1.

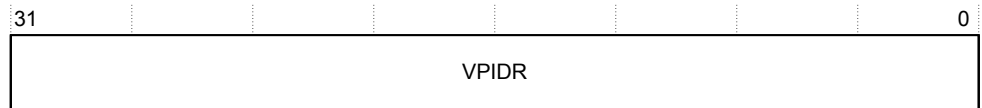


Figure B1-56 VPIDR_EL2 bit assignments

VPIDR, [31:0]

MIDR_EL1 value returned by Non-secure EL1 reads of the MIDR_EL1. The MIDR_EL1 description defines the subdivision of this value. See [Figure B1-35 MIDR_EL1 bit assignments on page B1-243](#).

To access the VPIDR_EL2:

```
MRS <Xt>, VPIDR_EL2 ; Read VPIDR_EL2 into Xt
MSR VPIDR_EL2, <Xt> ; Write Xt to VPIDR_EL2
```

Register access is encoded as follows:

Table B1-79 VPIDR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0000	0000	000

B1.85 Virtualization Translation Control Register, EL2

The VTCR_EL2 characteristics are:

Purpose

Controls the translation table walks required for the stage 2 translation of memory accesses from Non-secure EL0 and EL1, and holds cacheability and shareability information for the accesses.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	-	RW	RW	RW

Any of the bits in VTCR_EL2 are permitted to be cached in a TLB.

Configurations

There are no configuration notes.

Attributes

VTCR_EL2 is a 32-bit register.

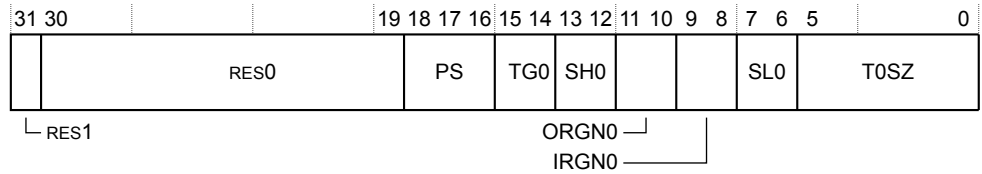


Figure B1-57 VTCR_EL2 bit assignments

[31]

Reserved, RES1.

[30:19]

Reserved, RES0.

PS, [18:16]

Physical Address Size. The possible values are:

0b000 32 bits, 4GB.

0b001 36 bits, 64GB.

0b010 40 bits, 1TB.

All other values are reserved.

TG0, [15:14]

Granule size for the corresponding VTTBR_EL2.

0b00 4KB.

0b10 16KB.

0b01 64KB.

0b11 Reserved.

All other values are not supported.

SH0, [13:12]

Shareability attribute for memory associated with translation table walks using VTTBR_EL2.

0b00 Non-shareable.

0b01 Reserved.

0b10 Outer Shareable.

0b11 Inner Shareable.

ORGN0, [11:10]

Outer cacheability attribute for memory associated with translation table walks using VTTBR_EL2.

- 0b00 Normal memory, Outer Non-cacheable.
- 0b01 Normal memory, Outer Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Outer Write-Through Cacheable.
- 0b11 Normal memory, Outer Write-Back no Write-Allocate Cacheable.

IRGN0, [9:8]

Inner cacheability attribute for memory associated with translation table walks using VTTBR_EL2.

- 0b00 Normal memory, Inner Non-cacheable.
- 0b01 Normal memory, Inner Write-Back Write-Allocate Cacheable.
- 0b10 Normal memory, Inner Write-Through Cacheable.
- 0b11 Normal memory, Inner Write-Back no Write-Allocate Cacheable.

SL0, [7:6]

Starting level of the VTCR_EL2 addressed region.

T0SZ, [5:0]

The size offset of the memory region addressed by VTTBR_EL2. The region size is $2^{(64-T0SZ)}$ bytes.

To access the VTCR_EL2:

```
MRS <Xt>, VTCR_EL2 ; Read VTCR_EL2 into Xt
MSR VTCR_EL2, <Xt> ; Write Xt to VTCR_EL2
```

Register access is encoded as follows:

Table B1-80 VTCR_EL2 access encoding

op0	op1	CRn	CRm	op2
11	100	0010	0001	010

Chapter B2

GIC registers

This chapter describes the GIC registers.

It contains the following sections:

- *B2.1 CPU interface register summary on page B2-282.*
- *B2.2 Active Priority Register on page B2-283.*
- *B2.3 CPU Interface Identification Register on page B2-284.*
- *B2.4 Virtual interface control register summary on page B2-285.*
- *B2.5 VGIC Type Register on page B2-286.*
- *B2.6 Virtual CPU interface register summary on page B2-287.*
- *B2.7 VM Active Priority Register on page B2-288.*
- *B2.8 VM CPU Interface Identification Register on page B2-289.*

B2.1 CPU interface register summary

Each CPU interface block provides the interface for a Cortex-A34 processor that interfaces with a GIC distributor within the system.

Each CPU interface provides a programming interface for:

- Enabling the signaling of interrupt requests by the CPU interface.
- Acknowledging an interrupt.
- Indicating completion of the processing of an interrupt.
- Setting an interrupt priority mask for the processor.
- Defining the preemption policy for the processor.
- Determining the highest priority pending interrupt for the processor.
- Generating SGIs.

For more information on the CPU interface, see the *ARM® Generic Interrupt Controller Architecture Specification*.

The following table lists the registers for the CPU interface.

All the registers in the following table are word-accessible. Registers not described in this table are RES0. See the *ARM® Generic Interrupt Controller Architecture Specification* for more information.

Table B2-1 CPU interface register summary

Offset	Name	Type	Reset	Description
0x0000	GICC_CTLR	RW	0x00000000	CPU Interface Control Register
0x0004	GICC_PMR	RW	0x00000000	Interrupt Priority Mask Register
0x0008	GICC_BPR	RW	0x00000002 (Secure) 0x00000003 (Non-secure)	Binary Point Register
0x000C	GICC_IAR	RO	-	Interrupt Acknowledge Register
0x0010	GICC_EOIR	WO	-	End Of Interrupt Register
0x0014	GICC_RPR	RO	0x000000FF	Running Priority Register
0x0018	GICC_HPPIR	RO	0x000003FF	Highest Priority Pending Interrupt Register
0x001C	GICC_ABPR	RW	0x00000003	Aliased Binary Point Register
0x0020	GICC_AIAR	RO	-	Aliased Interrupt Acknowledge Register
0x0024	GICC_AEOIR	WO	-	Aliased End of Interrupt Register
0x0028	GICC_AHPPIR	RO	0x000003FF	Aliased Highest Priority Pending Interrupt Register
0x00D0	GICC_APR0	RW	0x00000000	B2.2 Active Priority Register on page B2-283
0x00E0	GICC_NSAPR0	RW	0x00000000	Non-secure Active Priority Register
0x00FC	GICC_IIDR	RO	0x0024143B	B2.3 CPU Interface Identification Register on page B2-284
0x1000	GICC_DIR	WO	-	Deactivate Interrupt Register

B2.2 Active Priority Register

The GICC_APR0 characteristics are:

Purpose

Provides support for preserving and restoring state in power management applications.

Usage constraints

This register is banked to provide Secure and Non-secure copies. This ensures that Non-secure accesses do not interfere with Secure operation.

Configurations

Available in all configurations.

Attributes

See the register summary in [B2.1 CPU interface register summary on page B2-282](#).

The Cortex-A34 processor implements the GICC_APR0 according to the recommendations described in the *ARM Generic Interrupt Controller Architecture Specification*.

Table B2-2 Active Priority Register implementation

Number of group priority bits	Preemption levels	Minimum value of Secure GICC_BPR	Minimum legal value of Non-secure GICC_BPR	Active Priority Registers implemented	View of Active Priority Registers for Non-secure accesses
5	32	2	3	GICC_APR0 [31:0]	GICC_NSAPR0 [31:16] appears as GICC_APR0 [15:0]

B2.3 CPU Interface Identification Register

The GICC_IIDR characteristics are:

Purpose

Provides information about the implementer and revision of the CPU interface.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See the register summary in [B2.1 CPU interface register summary on page B2-282](#).

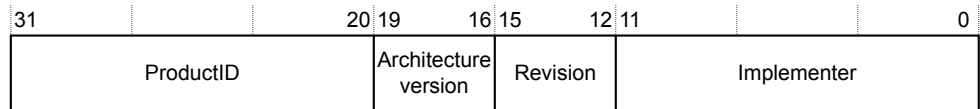


Figure B2-1 GICC_IIDR bit assignments

ProductID, [31:20]

Identifies the product:

0x002 Cortex-A34 processor.

Architecture version, [19:16]

Identifies the architecture version of the GIC CPU interface:

0x4 GICv4.

Revision, [15:12]

Identifies the revision number for the CPU interface:

0x1 r0p1.

Implementer, [11:0]

Contains the JEP106 code of the company that implements the CPU interface:

0x43B ARM.

B2.4 Virtual interface control register summary

The virtual interface control registers are management registers. Configuration software on the Cortex-A34 processor must ensure they are accessible only by a hypervisor, or similar software.

The following table describes the registers for the virtual interface control registers. All these registers are word-accessible. Registers not described in this table are RES0. See the *ARM® Generic Interrupt Controller Architecture Specification* for more information.

Table B2-3 Virtual interface control register summary

Offset	Name	Type	Reset	Description
0x000	GICH_HCR	RW	0x00000000	Hypervisor Control Register
0x004	GICH_VTR	RO	0x90000003	B2.5 VGIC Type Register on page B2-286
0x008	GICH_VMCR	RW	0x004C0000	Virtual Machine Control Register
0x010	GICH_MISR	RO	0x00000000	Maintenance Interrupt Status Register
0x020	GICH_EISR0	RO	0x00000000	End of Interrupt Status Registers
0x030	GICH_ELRSR0	RO	0x0000000F	Empty List Register Status Registers
0x0F0	GICH_APR0	RW	0x00000000	Active Priorities Register
0x100	GICH_LR0	RW	0x00000000	List Register 0
0x104	GICH_LR1	RW	0x00000000	List Register 1
0x108	GICH_LR2	RW	0x00000000	List Register 2
0x10C	GICH_LR3	RW	0x00000000	List Register 3

B2.5 VGIC Type Register

The GICH_VTR characteristics are:

Purpose

Holds information on number of priority bits, number of preemption bits, and number of List Registers implemented.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See the register summary in [B2.4 Virtual interface control register summary](#) on page B2-285.

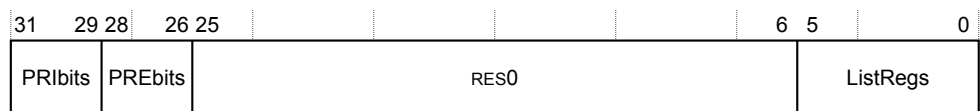


Figure B2-2 GICH_VTR bit assignments

PRIbits, [31:29]

Indicates the number of priority bits implemented, minus one:

0x4 Five bits of priority and 32 priority levels.

PREbits, [28:26]

Indicates the number of preemption bits implemented, minus one:

0x4 Five bits of preemption and 32 preemption levels.

[25:6]

Reserved, RES0.

ListRegs, [5:0]

Indicates the number of implemented List Registers, minus one:

0x3 Four List Registers.

B2.6 Virtual CPU interface register summary

The virtual CPU interface forwards virtual interrupts to a connected Cortex-A34 processor, subject to the normal GIC handling and prioritization rules.

The virtual interface control registers control virtual CPU interface operations. In particular, the virtual CPU interface uses the contents of the List registers to determine when to signal virtual interrupts. When a core accesses the virtual CPU interface, the List registers are updated. For more information on the virtual CPU interface, see the *ARM® Generic Interrupt Controller Architecture Specification*.

The following table describes the registers for the virtual CPU interface.

All the registers in the following table are word-accessible. Registers not described in this table are RES0. See the *ARM® Generic Interrupt Controller Architecture Specification* for more information.

Table B2-4 Virtual CPU interface register summary

Name	Type	Reset	Description
GICV_CTLR	RW	0x00000000	VM Control Register
GICV_PMR	RW	0x00000000	VM Priority Mask Register
GICV_BPR	RW	0x00000002	VM Binary Point Register
GICV_IAR	RO	-	VM Interrupt Acknowledge Register
GICV_EOIR	WO	-	VM End Of Interrupt Register
GICV_RPR	RO	0x000000FF	VM Running Priority Register
GICV_HPPIR	RO	0x000003FF	VM Highest Priority Pending Interrupt Register
GICV_ABPR	RW	0x00000003	VM Aliased Binary Point Register
GICV_AIAR	RO	-	VM Aliased Interrupt Acknowledge Register
GICV_AEOIR	WO	-	VM Aliased End of Interrupt Register
GICV_AHPPIR	RO	0x000003FF	VM Aliased Highest Priority Pending Interrupt Register
GICV_APR0	RW	0x00000000	B2.7 VM Active Priority Register on page B2-288
GICV_IIDR	RO	0x0024143B	B2.8 VM CPU Interface Identification Register on page B2-289
GICV_DIR	WO	-	VM Deactivate Interrupt Register

B2.7 VM Active Priority Register

GICV_APR0

For software compatibility, this register is present in the virtual CPU interface. However, in a virtualized system, it is not used when preserving and restoring state.

The GICV_APR0 characteristics are:

Purpose

For software compatibility, this register is present in the virtual CPU interface. However, in a virtualized system, it is not used when preserving and restoring state.

Usage constraints

Reading the content of this register and then writing the same values must not change any state because there is no requirement to preserve and restore state during a powerdown.

Configurations

Available in all configurations.

Attributes

See the register summary in [B2.6 Virtual CPU interface register summary on page B2-287](#).

The Cortex-A34 processor implements the GICV_APR0 as an alias of GICH_APR0.

B2.8 VM CPU Interface Identification Register

The GICV_IIDR characteristics are:

Purpose

Provides information about the implementer and revision of the virtual CPU interface.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See the register summary in *B2.6 Virtual CPU interface register summary on page B2-287*.

31	20	19	16	15	12	11	0
ProductID			Architecture version		Revision		Implementer

Figure B2-3 GICV_IIDR bit assignments

ProductID, [31:20]

Identifies the product:

0x002 Cortex-A34 processor.

Architecture version, [19:16]

Identifies the architecture version of the GIC CPU Interface:

0x4 GICv4.

Revision, [15:12]

Identifies the revision number for the CPU interface:

0x1 r0p1.

Implementer, [11:0]

Contains the JEP106 code of the company that implements the CPU interface:

0x43B ARM.

Chapter B3

Generic Timer registers

This chapter describes the Generic Timer registers.

It contains the following sections:

- [B3.1 AArch64 Generic Timer register summary on page B3-292.](#)

B3.1 AArch64 Generic Timer register summary

A set of Generic Timer registers are allocated within each core. The Generic Timer registers are either 32-bits wide or 64-bits wide.

The following table shows the AArch64 Generic Timer registers. See the *ARM Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for information about these registers.

Table B3-1 AArch64 Generic Timer registers

Name	Op0	CRn	Op1	CRm	Op2	Reset	Width	Description
CNTKCTL_EL1	3	c14	0	c1	0	-	32-bit	Counter-timer Kernel Control register The reset value for bits[9:8, 2:0] is 0b00000.
CNTFRQ_EL0			3	c0	0	UNK	32-bit	Counter-timer Frequency register
CNTPCT_EL0					1	UNK	64-bit	Counter-timer Physical Count register
CNTVCT_EL0					2	UNK	64-bit	Counter-timer Virtual Count register
CNTP_TVAL_EL0				c2	0	UNK	32-bit	Counter-timer Physical Timer TimerValue register
CNTP_CTL_EL0					1	-	32-bit	Counter-timer Physical Timer Control register The reset value for bit[0] is 0.
CNTP_CVAL_EL0					2	UNK	64-bit	Counter-timer Physical Timer CompareValue register
CNTV_TVAL_EL0				c3	0	UNK	32-bit	Counter-timer Virtual Timer TimerValue register
CNTV_CTL_EL0					1		32-bit	Counter-timer Virtual Timer Control register The reset value for bit[0] is 0.
CNTV_CVAL_EL0					2	UNK	64-bit	Counter-timer Virtual Timer CompareValue register
CNTVOFF_EL2			4	c0	3	UNK	64-bit	Counter-timer Virtual Offset register
CNTHCTL_EL2				c1	0	-	32-bit	Counter-timer Hypervisor Control register The reset value for bit[2] is 0 and for bits[1:0] is 0b11.
CNTHP_TVAL_EL2				c2	0	UNK	32-bit	Counter-timer Hypervisor Physical Timer TimerValue register
CNTHP_CTL_EL2					1		32-bit	Counter-timer Hypervisor Physical Timer Control register The reset value for bit[0] is 0.
CNTHP_CVAL_EL2					2	UNK	64-bit	Counter-timer Hypervisor Physical Timer CompareValue register
CNTPS_TVAL_EL1			7	c2	0	UNK	32-bit	Counter-timer Physical Secure Timer TimerValue register
CNTPS_CTL_EL1					1	-	32-bit	Counter-timer Physical Secure Timer Control register The reset value for bit[0] is 0.
CNTPS_CVAL_EL1					2	UNK	64-bit	Counter-timer Physical Secure Timer CompareValue register

Part C
Debug

Chapter C1

Debug

This chapter describes the debug features of the processor.

It contains the following sections:

- *C1.1 About debug methods on page C1-296.*
- *C1.2 Debug access on page C1-297.*
- *C1.3 Effects of resets on debug registers on page C1-298.*
- *C1.4 External access permissions to debug registers on page C1-299.*
- *C1.5 Debug events on page C1-300.*
- *C1.6 Debug memory map on page C1-301.*
- *C1.7 Debug signals on page C1-303.*
- *C1.8 Changing the authentication signals for debug on page C1-304.*

C1.1 About debug methods

The processor is part of a debug system and supports both self-hosted and external debug.

The following figure shows a typical external debug system.

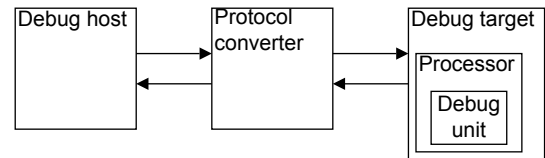


Figure C1-1 External debug system

Debug host

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. A device such as DSTREAM is required to convert between the two protocols.

Debug target

The lowest level of the system implements system support for the protocol converter to access the debug unit using the *Advanced Peripheral Bus (APB)* slave interface. An example of a debug target is a development system with a test chip or a silicon part with a processor.

Debug unit

Helps debugging software that is running on the processor:

- Hardware systems that are based on the processor.
- Operating systems.
- Application software.

With the debug unit, you can:

- Stop program execution.
- Examine and alter process and coprocessor state.
- Examine and alter memory and the state of the input or output peripherals.
- Restart the processor.

For self-hosted debug, the debug target runs additional debug monitor software that runs on the Cortex-A34 processor itself. This way, it does not require expensive interface hardware to connect a second host computer.

Related information

[C1.2 Debug access on page C1-297.](#)

C1.2 Debug access

The processor implements the ARMv8 Debug architecture and debug events. Accessing system registers allows the processor to access certain debug registers directly. The external debug interface enables both external and self-hosted debug agents to access debug registers.

The partitioning of debug register access is as follows:

Debug registers

Access is based on the system registers and is memory-mapped. You can access the debug register map using the APB slave port.

PMU

Access is based on the system registers and is memory-mapped. You can access the performance monitor registers using the APB slave port.

ETM

Access is memory-mapped.

CTI

Access is based on the debug registers and is memory-mapped.

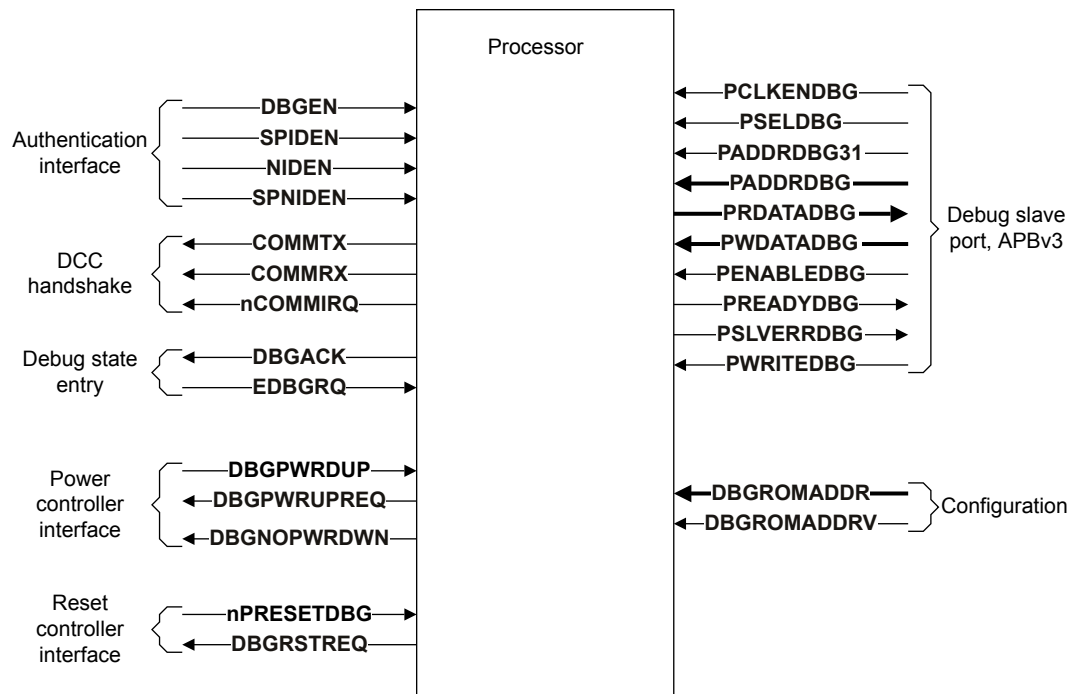


Figure C1-2 External debug interface

Related information

[Chapter C4 CTI on page C4-323.](#)

[Appendix A Signal Descriptions on page Appx-A-533.](#)

C1.3 Effects of resets on debug registers

Some of the processor reset signals affect the debug registers.

nCPUPORESET

Cold reset that covers reset of the processor logic and the integrated debug functionality.

The signal initializes the processor logic, including the debug, *Embedded Trace Macrocell* (ETM) trace unit, breakpoint, watchpoint logic, and performance monitors logic.

nCORERESET

Warm reset that covers reset of the processor logic.

The signal resets some of the debug and performance monitor logic.

nPRESETDBG

External debug reset that covers the resetting of the external debug interface and has no impact on the processor functionality.

The signal initializes the shared debug APB, *Cross Trigger Interface* (CTI), and *Cross Trigger Matrix* (CTM) logic.

Related information

[A3.3 Resets](#) on page A3-46.

[Appendix A Signal Descriptions](#) on page Appx-A-533.

C1.4 External access permissions to debug registers

External access permission to the debug registers is subject to the conditions at the time of the access.

The following table describes the processor response to accesses to the debug registers.

Table C1-1 Conditions on external register access to debug registers

Name	Condition	Description
Off	EDPRSR.PU is 0	The processor power domain is completely off or in a low-power state in which the processor power domain registers cannot be accessed. If debug power is off, then all external debug and memory-mapped register accesses return an error.
DLK	EDPRSR.DLK is 1	OS Double Lock is locked.
OSLK	OSLSR_EL1.OSLK is 1	OS Lock is locked.
EDAD	AllowExternalDebugAccess() == FALSE	External debug access is disabled. When an error is returned because of an EDAD condition code, the highest priority error condition, EDPRSR.SDAD is set to 1. Otherwise SDAD is unchanged.
SLK	Memory-mapped interface only	Software lock is locked. For the external debug interface, ignore this column.
Default	-	None of the conditions apply, normal access.

The following table shows an example of external register condition codes for access to a debug register. To determine the access permission for the register, scan the columns from left to right. Stop at the first column a condition is true, the entry gives the access permission of the register and scanning stops.

Table C1-2 Code example for the conditions on external register access to debug registers

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	RO/WI	RO

C1.5 Debug events

A debug event can be either a software debug event or a halting debug event. A core responds to a debug event in one of the following ways: ignores it, takes a debug exception, or enters debug state.

In the processor, watchpoint debug events are always synchronous. Memory hint instructions and cache clean operations, except DC ZVA, DC IVAC, and DCIMVAC, 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. For watchpoint debug events, except those resulting from cache maintenance operations, the value reported in DFAR is guaranteed to be no lower than the address of the watchpointed location rounded down to a multiple of 16 bytes.

The powerup reset signal, **nCPUPORESET**, sets the Debug OS Lock. For the debug events and debug register accesses to operate normally, the Debug OS Lock must be cleared.

Related information

[A3.3 Resets](#) on page A3-46.

[A.4 Reset signals](#) on page Appx-A-537.

ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile.

C1.6 Debug memory map

The basic memory map supports up to four cores in the cluster. You can configure the mapping as a v8 or as a v7 Debug memory map.

The following table shows the address mapping for the debug APB components when you configure them for a v8 Debug memory map. Each component in the table requires 4KB and uses the bottom 4KB of each 64KB region. The remaining 60KB of each region is reserved. The table indicates the mapped component if it is present, otherwise the field is reserved.

Table C1-3 Address mapping for APB components in a v8 Debug memory map

Address offset [21:0]	Mapped to
0x000000 - 0x000FFF	APB ROM table for the processor
0x010000 - 0x010FFF	Core 0 Debug
0x020000 - 0x020FFF	Core 0 CTI
0x030000 - 0x030FFF	Core 0 PMU
0x040000 - 0x040FFF	Core 0 Trace
0x041000 - 0x10FFFF	Reserved
0x110000 - 0x110FFF	Core 1 Debug
0x120000 - 0x120FFF	Core 1 CTI
0x130000 - 0x130FFF	Core 1 PMU
0x140000 - 0x140FFF	Core 1 Trace
0x141000 - 0x20FFFF	Reserved
0x210000 - 0x210FFF	Core 2 Debug
0x220000 - 0x220FFF	Core 2 CTI
0x230000 - 0x230FFF	Core 2 PMU
0x240000 - 0x240FFF	Core 2 Trace
0x241000 - 0x30FFFF	Reserved
0x310000 - 0x310FFF	Core 3 Debug
0x320000 - 0x320FFF	Core 3 CTI
0x330000 - 0x330FFF	Core 3 PMU
0x340000 - 0x340FFF	Core 3 Trace
0x341000 - 0x3FFFFFFF	Reserved

The following table shows the address mapping for the debug components when you configure them for a v7 Debug memory map. The table indicates the mapped component if it is present, otherwise the field is reserved.

Table C1-4 Address mapping for APB components in a v7 Debug memory map

Address offset [21:0]	Mapped to
0x00000 - 0x00FFF	APB ROM table for the processor
0x01000 - 0x07FFF	Reserved for other debug components
0x08000 - 0x0FFFF	Reserved for future expansion
0x10000 - 0x10FFF	Core 0 Debug
0x11000 - 0x11FFF	Core 0 PMU
0x12000 - 0x12FFF	Core 1 Debug
0x13000 - 0x13FFF	Core 1 PMU
0x14000 - 0x14FFF	Core 2 Debug
0x15000 - 0x15FFF	Core 2 PMU
0x16000 - 0x16FFF	Core 3 Debug
0x17000 - 0x17FFF	Core 3 PMU
0x18000 - 0x18FFF	Core 0 CTI
0x19000 - 0x19FFF	Core 1 CTI
0x1A000 - 0x1AFFF	Core 2 CTI
0x1B000 - 0x1BFFF	Core 3 CTI
0x1C000 - 0x1CFFF	Core 0 Trace
0x1D000 - 0x1DFFF	Core 1 Trace
0x1E000 - 0x1EFFF	Core 2 Trace
0x1F000 - 0x1FFFF	Core 3 Trace

C1.7 Debug signals

The **DBGPWRDUP** and **DBGL1RSTDISABLE** signals are subject to particular rules.

You must set the **DBGPWRDUP** signal LOW before removing power to the processor domain. After power is restored to the processor domain, the **DBGPWRDUP** signal must be asserted HIGH. The EDPRSR.PU bit reflects the value of this **DBGPWRDUP** signal. **DBGPWRDUP** must be tied HIGH if the particular implementation does not support separate processor and SCU power domains.

When you set it HIGH, the **DBGL1RSTDISABLE** input signal disables the automatic, hardware-controlled invalidation with **nCORERESET** or **nCPUPORESET** of the L1 data cache after the processor is reset. You must use **DBGL1RSTDISABLE** only to debug a reset that an external watchdog triggered. This signal makes the contents of the L1 data cache from before the reset observable after the reset. If reset is asserted while an L1 data cache eviction or L1 data cache fetch is performed, the accuracy of those cache entries is not guaranteed. You must not use the **DBGL1RSTDISABLE** signal to disable the automatic, hardware controlled invalidation of the L1 data cache in normal processor powerup sequences. This is because there is no guarantee that the L1 data cache invalidation sequence is synchronized to the duplicate L1 tags in the SCU. The **DBGL1RSTDISABLE** signal applies to all cores in the cluster. Each core samples the signal when **nCORERESET** or **nCPUPORESET** is asserted. If the functionality offered by the **DBGL1RSTDISABLE** input signal is not required, the input must be tied to LOW.

Related information

[A.14 Debug signals on page Appx-A-557.](#)

C1.8 Changing the authentication signals for debug

The **NIDEN**, **DBGEN**, **SPIDEN**, and **SPNIDEN** input signals are either tied off to some fixed value or controlled by some external device. If software running on the processor has control over an external device that drives the authentication signals, it must change the signal value using the specified procedure.

Procedure

1. Execute an implementation-specific sequence of instructions to change the signal value. For example, a single STR instruction might write certain values to a control register in a system peripheral.
2. If step 1 on page C1-304 involves any memory operation, issue a DSB instruction.
3. Issue an ISB instruction or exception entry or exception return.
4. Poll the DBGAUTHSTATUS_EL1 register to check whether the processor has already detected the changed value of these signals. This check is required because the system might not issue the signal change to the processor until several cycles after the DSB instruction completes.

Postrequisites

Software cannot perform debug or analysis operations that depend on the new value of the authentication signals until this procedure is complete. The same rules apply when the debugger has control of the processor through the Instruction Transfer Register, EDITR, while in debug state. You can determine the relevant combinations of the **DBGEN**, **NIDEN**, **SPIDEN**, and **SPNIDEN** values by polling DBGAUTHSTATUS_EL1.

Related information

[A.14 Debug signals on page Appx-A-557.](#)

Chapter C2

PMU

This chapter describes the *Performance Monitor Unit* (PMU) of the processor.

It contains the following sections:

- *C2.1 About the PMU* on page C2-306.
- *C2.2 External register access permissions to the PMU registers* on page C2-307.
- *C2.3 Performance monitoring events* on page C2-308.
- *C2.4 PMU interrupts* on page C2-312.
- *C2.5 Exporting PMU events* on page C2-313.

C2.1 About the PMU

The processor includes performance monitors that enable you to gather various statistics on the operation of the processor and its memory system during runtime. They provide useful information that you can use when debugging or profiling code.

The PMU provides six counters. Each counter can count any of the events available in the processor. The absolute counts that the PMU records might vary because of pipeline effects. This variability only has an impact on the operation of the PMU when a counter is enabled for a short time.

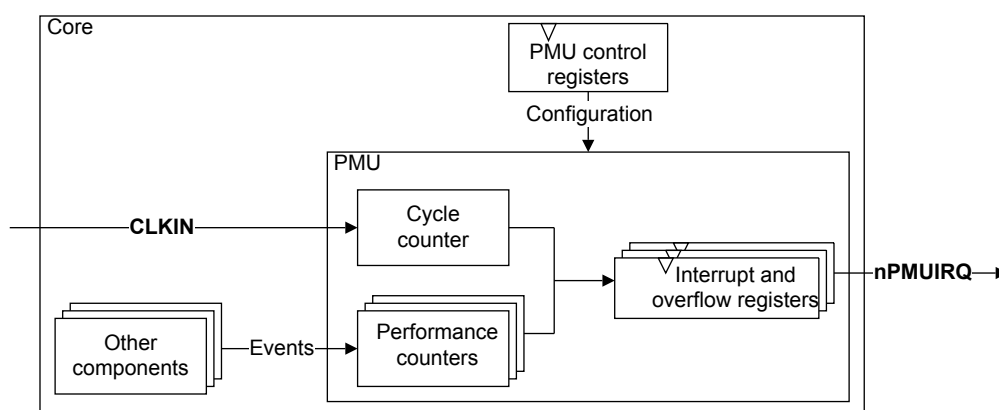


Figure C2-1 PMU block diagram

Event interface

Events from all other units from across the design are provided to the PMU.

System register and APB interface

You can program the PMU registers using the system registers or external APB interface.

Counters

The PMU has six 32-bit performance counters and one 64-bit cycle counter. The performance counters increment when they are enabled based on events.

PMU register interfaces

The processor supports access to the performance monitor registers from the internal system register interface or external debug interface.

Related information

[C2.3 Performance monitoring events on page C2-308.](#)

[C4.2 Cross-trigger inputs and outputs on page C4-325.](#)

C2.2 External register access permissions to the PMU registers

External access permission to the PMU registers is subject to conditions at the time of the access.

The following table describes the processor response to accesses through the external debug interface.

Table C2-1 Conditions on external register access to PMU

Name	Condition	Description
Off	EDPRSR.PU is 0	Processor power domain is completely off or in a low-power state where the processor power domain registers cannot be accessed.
DLK	EDPRSR.DLK is 1	OS Double Lock is locked.
OSLK	OSLSR_EL1.OSLK is 1	OS Lock is locked.
EPMAD	AllowExternalPMUAccess() == FALSE	External performance monitors access is disabled. When an error is returned because of an EPMAD condition code, and it is the highest priority error condition, EDPRSR.SPMAD is set to 1. Otherwise SPMAD is unchanged.
SLK	Memory-mapped interface only	Software lock is locked. For the external debug interface, ignore this column.
Default	-	None of the conditions apply, normal access.

To determine the access permission for the register, scan the columns from left to right in the register usage constraints table. An example is shown in [Table C2-2 Example for external register condition code on page C2-307](#). Stop at the first column in which the condition is true. The entry gives the register access permission and scanning stops.

Table C2-2 Example for external register condition code

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO/WI	RO

C2.3 Performance monitoring events

The PMU monitors events in the processor and uses reference numbers for significant ones.

The following table shows the bit position of each event on the event bus. Event reference numbers that are not listed are reserved.

Table C2-3 Performance monitoring events

Number	Event mnemonic	PMU event bus to external	PMU event bus to trace	Event name
0x00	SW_INCR	-	-	Software increment. The register is incremented only on writes to the Software Increment Register.
0x01	L1I_CACHE_REFILL	[0]	[0]	L1 Instruction cache refill.
0x02	L1I_TLB_REFILL	[1]	[1]	L1 Instruction TLB refill.
0x03	L1D_CACHE_REFILL	[2]	[2]	L1 Data cache refill.
0x04	L1D_CACHE	[3]	[3]	L1 Data cache access.
0x05	L1D_TLB_REFILL	[4]	[4]	L1 Data TLB refill.
0x06	LD_RETIRED	[5]	[5]	Instruction that is architecturally executed, condition check pass - load.
0x07	ST_RETIRED	[6]	[6]	Instruction that is architecturally executed, condition check pass - store.
0x08	INST_RETIRED	[7]	[7]	Instruction that is architecturally executed.
-	-	[8]	[8]	Two instructions are architecturally executed. Counts every cycle in which two instructions are architecturally retired. Event 0x08, INST_RETIRED, always counts when this event counts.
0x09	EXC_TAKEN	[9]	[9]	Exception taken.
0x0A	EXC_RETURN	[10]	[10]	Exception return.
0x0B	CID_WRITE_RETIRED	[11]	[11]	Change to Context ID retired.
0x0C	PC_WRITE_RETIRED	[12]	[12]	Instruction that is architecturally executed, condition check pass, software change of the PC.
0x0D	BR_IMMED_RETIRED	[13]	[13]	Instruction that is architecturally executed, immediate branch.
0x0E	BR_RETURN_RETIRED	-	-	Instruction that is architecturally executed, condition code check pass, procedure return.
0x0F	UNALIGNED_LDST_RETIRED	[14]	[14]	Instruction that is architecturally executed, condition check pass, unaligned load or store.
0x10	BR_MIS_PRED	[15]	[15]	Mispredicted or not predicted branch that is speculatively executed.
0x11	CPU_CYCLES	-	-	Cycle.
0x12	BR_PRED	[16]	[16]	Predictable branch that is speculatively executed.
0x13	MEM_ACCESS	[17]	[17]	Data memory access.

Table C2-3 Performance monitoring events (continued)

Number	Event mnemonic	PMU event bus to external	PMU event bus to trace	Event name
0x14	L1I_CACHE	[18]	[18]	L1 Instruction cache access.
0x15	L1D_CACHE_WB	[19]	[19]	L1 Data cache writeback.
0x16	L2D_CACHE	[20]	[20]	L2 Data cache access.
0x17	L2D_CACHE_REFILL	[21]	[21]	L2 Data cache refill.
0x18	L2D_CACHE_WB	[22]	[22]	L2 Data cache write-back.
0x19	BUS_ACCESS	-	-	Bus access.
0x1A	MEMORY_ERROR	-	-	Local memory error.
0x1D	BUS_CYCLES	-	-	Bus cycle.
0x1E	CHAIN	-	-	Odd performance counter chain mode.
0x60	BUS_ACCESS_LD	-	-	Bus access - Read.
0x61	BUS_ACCESS_ST	-	-	Bus access - Write.
0x7A	BR_INDIRECT_SPEC	-	-	Branch that is speculatively executed - Indirect branch.
0x86	EXC_IRQ	-	-	Exception taken, IRQ.
0x87	EXC_FIQ	-	-	Exception taken, FIQ.
0xC0	-	-	-	External memory request.
0xC1	-	-	-	Non-cacheable external memory request.
0xC2	-	-	-	Linefill because of prefetch.
0xC4	-	-	-	Entering read allocate mode.
0xC5	-	-	-	Read allocate mode.
0xC7	-	-	-	Data Write operation that stalls the pipeline because the store buffer is full.
0xC8	-	-	-	SCU Snooped data from another core for this core.
0xC9	-	-	-	Conditional branch that is executed.
0xCA	-	-	-	Indirect branch that is mispredicted.
0xCB	-	-	-	Indirect branch that is mispredicted because of address miscompare.
0xCC	-	-	-	Conditional branch that is mispredicted.
0xD0	-	[23]	[23]	L1 Instruction Cache (data or tag) memory error.
0xD1	-	[24]	[24]	L1 Data Cache (data, tag, or dirty) memory error, correctable or non-correctable.
0xD2	-	[25]	[25]	TLB memory error.
0xE0	-	-	-	Attributable Performance Impact Event. Counts every cycle that the DPU IQ is empty and that is not because of a recent micro-TLB miss, an instruction cache miss or a pre-decode error.

Table C2-3 Performance monitoring events (continued)

Number	Event mnemonic	PMU event bus to external	PMU event bus to trace	Event name
0xE1	-	-	-	Attributable Performance Impact Event. Counts every cycle the DPU IQ is empty and there is an instruction cache miss being processed.
0xE2	-	-	-	Attributable Performance Impact Event. Counts every cycle the DPU IQ is empty and there is an instruction micro-TLB miss being processed.
0xE3	-	-	-	Attributable Performance Impact Event. Counts every cycle the DPU IQ is empty and there is a pre-decode error being processed.
0xE4	-	-	-	Attributable Performance Impact Event. Counts every cycle there is an interlock that is not because of an Advanced SIMD or floating-point instruction, and not because of a load/store instruction waiting for data to calculate the address in the AGU. Stall cycles because of a stall in Wr, typically awaiting load data, are excluded.
0xE5	-	-	-	Attributable Performance Impact Event. Counts every cycle there is an interlock that is because of a load/store instruction waiting for data to calculate the address in the AGU. Stall cycles because of a stall in Wr, typically awaiting load data, are excluded.
0xE6	-	-	-	Attributable Performance Impact Event. Counts every cycle there is an interlock that is because of an Advanced SIMD or floating-point instruction. Stall cycles because of a stall in the Wr stage, typically awaiting load data, are excluded.
0xE7	-	-	-	Attributable Performance Impact Event Counts every cycle there is a stall in the Wr stage because of a load miss.
0xE8	-	-	-	Attributable Performance Impact Event. Counts every cycle there is a stall in the Wr stage because of a store.
-	-	[26]	[26]	L2 (data or tag) memory error, correctable or non-correctable.
-	-	[27]	[27]	SCU snoop filter memory error, correctable or non-correctable.

Table C2-3 Performance monitoring events (continued)

Number	Event mnemonic	PMU event bus to external	PMU event bus to trace	Event name
-	-	[28]	-	Advanced SIMD and floating-point retention active.
-	-	[29]	-	Core retention active.

C2.4 PMU interrupts

The processor asserts the **nPMUIRQ** signal when an interrupt occurs that the PMU generated.

You can route this signal to an external interrupt controller for prioritization and masking. It is the only mechanism that signals this interrupt to the processor.

This interrupt is also driven as a trigger input to the CTI.

Related information

[C4.2 Cross-trigger inputs and outputs on page C4-325.](#)

C2.5 Exporting PMU events

Some of the PMU events are exported to the ETM trace unit and the *Cross Trigger Interface (CTI)* to enable them to be monitored. Furthermore, the processor exports some PMU events on the **PMUEVENT** bus to external hardware.

Related information

[Chapter C3 ETM on page C3-315.](#)

[Chapter C4 CTI on page C4-323.](#)

Chapter C3

ETM

This chapter describes the *Embedded Trace Macrocell* (ETM) of the processor.

It contains the following sections:

- [C3.1 About the ETM](#) on page C3-316.
- [C3.2 Configuration options for the ETM unit and trace resources](#) on page C3-318.
- [C3.3 Resetting the ETM](#) on page C3-320.
- [C3.4 Programming and reading ETM trace unit registers](#) on page C3-321.

C3.1 About the ETM

The ETM trace unit is a build-time configuration option. This module performs real-time instruction flow tracing that complies with the ETM architecture. As a CoreSight component, it is part of the ARM real-time debug solution.

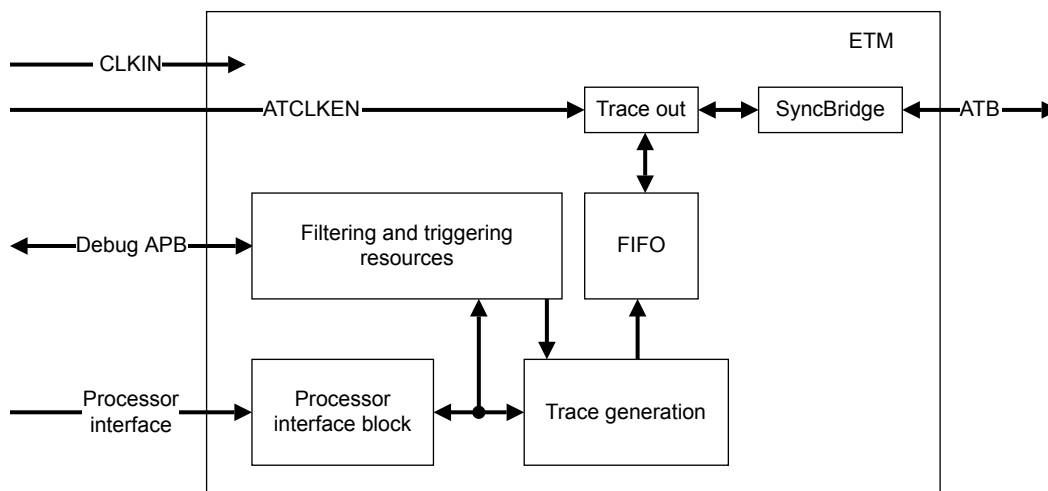


Figure C3-1 ETM functional blocks

Filtering and triggering resources

You can limit the amount of trace data that the ETM generates through filtering. For example, you can configure the ETM to generate trace only in a certain address range. More complicated filtering options, in the style of a logic analyzer, are also available.

The ETM trace unit can also generate a trigger signal to the Trace Capture Device to stop capturing trace.

Processor interface

Monitors the behavior of the processor and generates P0 elements that are executed instructions and exceptions that the ETM traces in program order.

Trace generation

Generates various trace packets that are based on P0 elements.

FIFO

The ETM generates trace in a highly compressed form. The FIFO can flatten trace bursts. When it becomes full, it signals overflow so that the trace generation logic does not generate any new trace until the FIFO becomes empty. The period without trace generation results in a gap in the trace in the debugger view.

Trace out

Trace from FIFO is output on the synchronous ATB interface.

Syncbridge

The ATB interface from the trace out block goes through an ATB synchronous bridge.

Interaction with the *Performance Monitoring Unit* (PMU)

The processor includes a PMU that enables counting events, such as cache misses, over a period. All PMU architectural events are available to the ETM trace unit through the extended input facility. The ETM trace unit uses four extended external input selectors to access the PMU events. Each selector can independently select one of the PMU events, which is then active for the cycles where the relevant events occur. Any ETM event register can access the selected event.

The processor supports only a memory-mapped interface to trace registers.

All trace register accesses through the external debug interface behave as if the processor power domain is powered down when debug double lock is set.

Related information

ARM® CoreSight Architecture Specification.
Chapter C2 PMU on page C2-305.

C3.2 Configuration options for the ETM unit and trace resources

The ETM unit is configurable. The processor implements options for the ETM unit and its resources.

Table C3-1 Configuration of trace generation

Description	Configuration
Instruction address size in bytes	8
Data address size in bytes	0
Data value size in bytes	0
Virtual Machine ID size in bytes	1
Context ID size in bytes	4
Support for conditional instruction tracing	Not implemented
Support for tracing of data	Not implemented
Support for tracing of load and store instructions as P0 elements	Not implemented
Support for cycle counting in the instruction trace	Implemented
Support for branch broadcast tracing	Implemented
Exception levels implemented in Non-secure state	EL2, EL1, EL0
Exception levels implemented in Secure state	EL3, EL1, EL0
Number of events supported in the trace	4
Return stack support	Implemented
Tracing of SError exception support	Implemented
Instruction trace cycle counting minimum threshold	1
Size of Trace ID	7 bits
Synchronization period support	Read-write
Global timestamp size	64 bits
Number of cores available for tracing	1
ATB trigger support	Implemented
Low-power behavior override	Implemented
Stall control support	Implemented
Support for no overflows in the trace	Not implemented

Table C3-2 Configuration of trace resources

Description	Configuration
Number of resource selection pairs implemented	8
Number of external input selectors implemented	4
Number of external inputs implemented	30, 4 CTI + 26 PMU
Number of counters implemented	2
Reduced function counter implemented	Not implemented

Table C3-2 Configuration of trace resources (continued)

Description	Configuration
Number of sequencer states implemented	4
Number of Virtual Machine ID comparators implemented	1
Number of Context ID comparators implemented	1
Number of address comparator pairs implemented	4
Number of single-shot comparator controls	1
Number of processor comparator inputs implemented	0
Data address comparisons implemented	Not implemented
Number of data value comparators implemented	0

C3.3 Resetting the ETM

The reset for the ETM trace unit is the same as a cold reset for the processor. If the ETM trace unit is reset, tracing stops until the ETM trace unit is reprogrammed and re-enabled.

A warm reset of the processor does not reset the ETM trace unit. Therefore it is possible to trace through warm processor reset. However, if the processor is reset using warm reset, the trace unit might not be able to trace the last few instructions before the reset.

C3.4 Programming and reading ETM trace unit registers

You program and read the ETM trace unit registers using the Debug APB interface.

The processor does not have to be in the debug state while you program the ETM trace unit registers.

When you are programming the ETM trace unit registers, you must enable all the changes at the same time. Otherwise if you reprogram the counter, it might start to count based on incorrect events before the correct setup is in place for the trigger condition.

To disable the ETM trace unit, use the TRCPRGCTLR.EN bit.

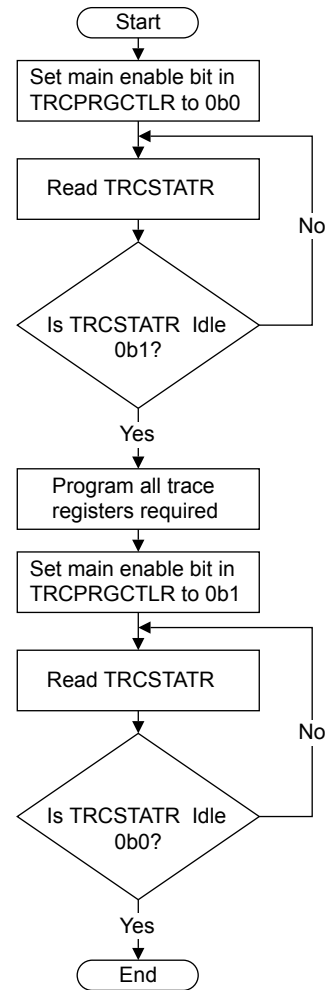


Figure C3-2 Programming ETM trace unit registers

Related information

[C10.2 Programming Control Register on page C10-426.](#)

[C10.3 Status Register on page C10-427.](#)

Chapter C4

CTI

This chapter describes the cross-trigger components of the processor.

It contains the following sections:

- [C4.1 About the cross-trigger on page C4-324.](#)
- [C4.2 Cross-trigger inputs and outputs on page C4-325.](#)

C4.1 About the cross-trigger

The *Cross-Trigger Interface* (CTI) enables the debug logic, ETM trace unit, and PMU to interact with each other and with other CoreSight components. For example, you configure the CTI to generate an interrupt when the ETM trace unit trigger event occurs.

The single external cross-trigger channel interface of the processor connects to the CTI of each core through a *Cross Trigger Matrix* (CTM). Trigger inputs and trigger outputs connect debug components in the processor and CoreSight CTI blocks. The external CTM output is driven by the OR of the internal CTI outputs. Each internal CTI input is driven by the OR of the other internal CTI outputs and the external CTM input.

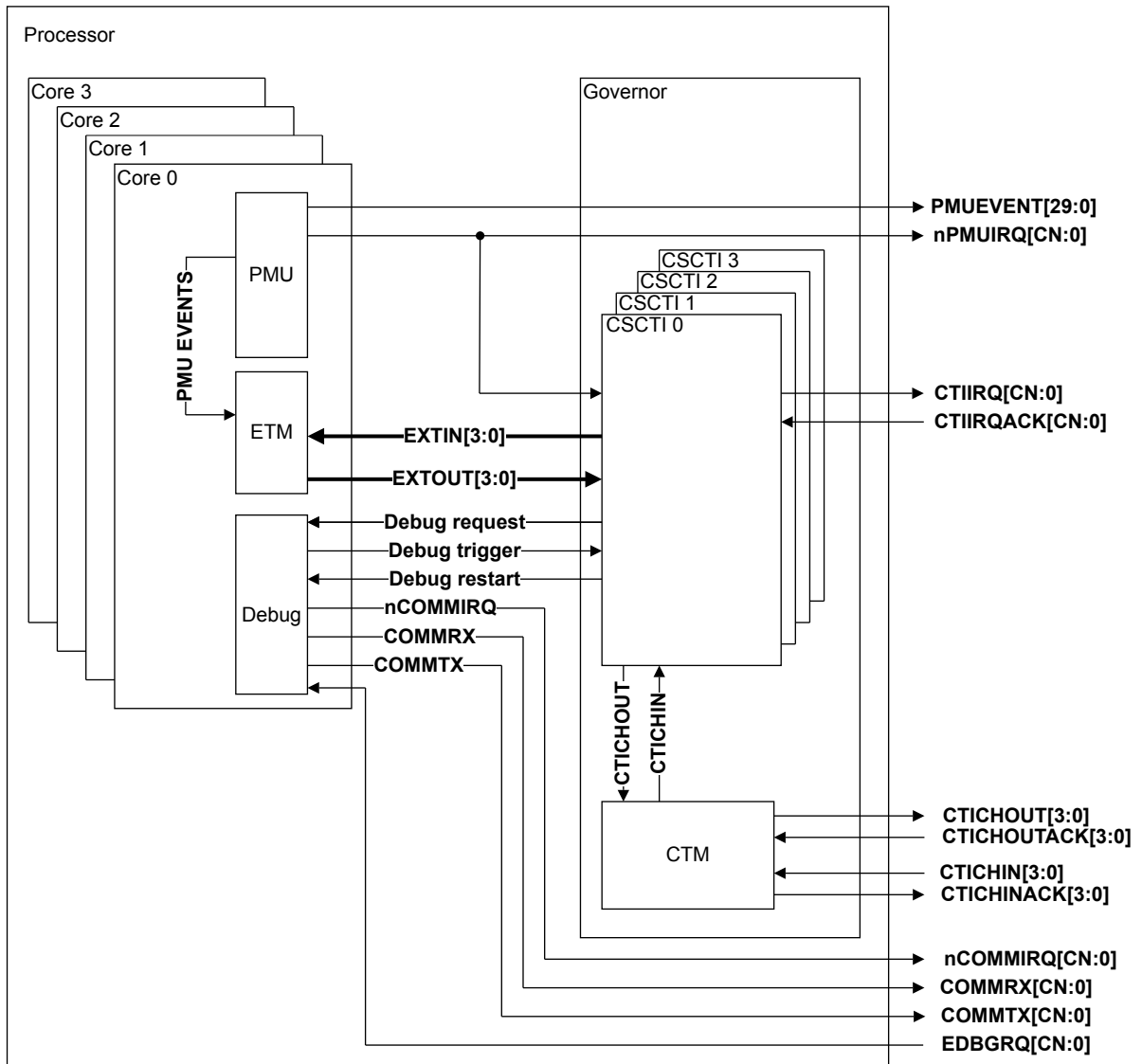


Figure C4-1 Cross-trigger components

C4.2 Cross-trigger inputs and outputs

Outputs from the PMU, the ETM, and the debug subsystem are cross-trigger inputs to the processor CTI. The CTI then generates cross-trigger outputs to other components in the SoC.

Table C4-1 Cross-trigger inputs

CTI input	Name	Description
0	DBGTRIGGER , pulsed	Pulsed on entry to debug state.
1	PMUIRQ	PMU-generated interrupt. This signal is the same as nPMUIRQ with inverted polarity.
2	-	-
3	-	-
4	EXTOUT[0]	Output from the ETM unit of Core<N>.
5	EXTOUT[1]	
6	EXTOUT[2]	
7	EXTOUT[3]	

Table C4-2 Cross-trigger outputs

CTI output	Name	Description
0	EDBGRQ	Causes the processor to enter debug state
1	DBGRESTART	Causes the processor to exit debug state
2	CTIIRQ	CTI interrupt
3	-	-
4	EXTIN[0]	ETM trace unit external input
5	EXTIN[1]	ETM trace unit external input
6	EXTIN[2]	ETM trace unit external input
7	EXTIN[3]	ETM trace unit external input

Chapter C5

Direct access to internal memory

This chapter describes the direct access to internal memory that caches and TLBs use.

It contains the following sections:

- *C5.1 About direct access to internal memory on page C5-328.*
- *C5.2 Encoding for tag and data in the L1 instruction cache on page C5-329.*
- *C5.3 Encoding for tag and data in the L1 data cache on page C5-330.*
- *C5.4 Encoding for the main TLB RAM on page C5-332.*
- *C5.5 Encoding for walk cache on page C5-337.*
- *C5.6 Encoding for IPA cache on page C5-338.*

C5.1 About direct access to internal memory

System registers provide access to the internal memory that the caches and TLBs use. This functionality can be useful when investigating issues where the coherency between the data in the cache and data in system memory is broken.

The appropriate memory block and location are selected using write-only registers and the data is read from read-only registers. These operations are available only in EL3. In all other modes, executing these instructions results in an Undefined Instruction exception.

Table C5-1 AArch64 registers used to access internal memory

Function	Access	Operation	Rd Data
Data Register 0	Read-only	MRS <Xd>, S3_3_c15_c0_0	Data
Data Register 1	Read-only	MRS <Xd>, S3_3_c15_c0_1	Data
Data Register 2	Read-only	MRS <Xd>, S3_3_c15_c0_2	Data
Data Register 3	Read-only	MRS <Xd>, S3_3_c15_c0_3	Data
Data Cache Tag Read Operation Register	Write-only	MSR S3_3_c15_c2_0, <Xd>	Set/Way
Instruction Cache Tag Read Operation Register	Write-only	MSR S3_3_c15_c2_1, <Xd>	Set/Way
Data Cache Data Read Operation Register	Write-only	MSR S3_3_c15_c4_0, <Xd>	Set/Way/Offset
Instruction Cache Data Read Operation Register	Write-only	MSR S3_3_c15_c4_1, <Xd>	Set/Way/Offset
TLB Data Read Operation Register	Write-only	MSR S3_3_c15_c4_2, <Xd>	Index/Way

Related information

[C5.4 Encoding for the main TLB RAM on page C5-332.](#)

C5.2 Encoding for tag and data in the L1 instruction cache

The following table shows the format of the Instruction Cache Tag Read Operation Register and the Instruction Cache Data Read Operation Register.

The set-index range parameter (S) is determined by the following formula:

$$S = \log_2(\text{size of the instruction cache in bytes} / 2)$$

Table C5-2 Instruction cache tag and data location encoding

Bit field	Description
[31]	Cache Way
[30:S]	Unused
[S-1:6]	Set index
[5:2]	Line offset
[1:0]	Unused

The following table shows the format of the information in Data Register 0 following an Instruction Cache Tag Read Operation.

Table C5-3 Instruction cache tag data format

Bits	Description
[31:30]	Unused.
[29]	Valid and set mode: 0b0 A64. 0b1 Invalid.
[28]	Non-secure state (NS).
[27:0]	Tag address.

The Instruction Cache Data Read Operation returns two entries from the cache in Data Register 0 and Data Register 1 corresponding to the 16-bit aligned offset in the cache line:

Data Register 0 Bits[19:0] data from cache offset+ **0b00**.

Data Register 1 Bits[19:0] data from cache offset+ **0b10**.

In A64 state these two fields combined always represent a single predecoded instruction.

C5.3 Encoding for tag and data in the L1 data cache

The following table shows the format of the Data Cache Tag Read Operation Register and the Data Cache Data Read Operation Register. The Data Cache Tag Read Operation and the Data Cache Data Read Operation use the same encoding but the latter includes an additional field to locate the appropriate doubleword in the cache line.

The set-index range parameter (S) is determined by the following formula:

$$S = \log_2(\text{size of the data cache in bytes}/4).$$

Table C5-4 Data cache tag and data location encoding

Bit field	Description
[31:30]	Cache way
[29:S]	Unused
[S-1:6]	Set index
[5:3]	Cache doubleword data offset (Data Cache Data Read Operation Register only)
[2:0]	Unused, RAZ.

The Data Cache Tag Read Operation returns 64 bits of data in Data Register 0 and Data Register 1. This includes the tag information, MOESI coherency state, outer attributes, and valid bit, for the selected cache line. The following table shows the format of the return value. The Cortex-A34 processor encodes the 4-bit MOESI coherency state across two fields of Data Register 0 and Data Register 1.

Table C5-5 Data cache tag data format

Register	Bit field	Description
Data Register 1	[31]	Parity bit if ECC is implemented, otherwise RES0.
Data Register 1	[30:29]	Partial MOESI State, from tag RAM. See Table C5-6 MOESI state on page C5-331 .
Data Register 1	[28]	Non-secure state (NS).
Data Register 1	[27:0]	Tag Address [39:12].
Data Register 0	[31]	Tag Address [11].
Data Register 0	[30:5]	Reserved, RES0.
Data Register 0	[4]	Parity bit if ECC is implemented, otherwise RES0.
Data Register 0	[3]	Dirty copy bit if ECC is implemented, otherwise RES0.
Data Register 0	[2]	Outer Allocation Hint.
Data Register 0	[1]	Outer Shareability, from Dirty RAM.
Data Register 0	[0]	Partial MOESI state, from Dirty RAM. See Table C5-6 MOESI state on page C5-331 .

The Data Cache Data Read Operation returns two entries from the cache in Data Register 0 and Data Register 1 corresponding to the 16-bit aligned offset in the cache line:

Data Register 0 Bits[31:0] data from cache offset+ 0b000.

Data Register 1 Bits[31:0] data from cache offset+ 0b100.

Table C5-6 MOESI state

Tag RAM partial MOESI bits	Dirty RAM partial MOESI bits	MOESI state
00	x	Invalid (I)
01	0	SharedClean (S)
	1	SharedDirty (O)
1x	0	UniqueClean (E)
	1	UniqueDirty (M)

Related information

[A5.2 Coherency between data caches with the MOESI protocol on page A5-71.](#)

C5.4 Encoding for the main TLB RAM

The Cortex-A34 processor unified TLB is built from a 2-way set-associative RAM based structure. To read the individual entries into the data registers, software must write to the TLB Data Read Operation Register.

The following table shows the format of the TLB Data Read Operation Register.

Table C5-7 Location encoding for the TLB Data Read Operation Register

Bits	Description
[31]	Unused
[30]	TLB way
[29:9]	Unused
[8:0]	TLB index 0-255 Main TLB RAM 256-287 Walk cache RAM 288-319 IPA cache RAM 320-511 Unused

The TLB Read Data Operation returns the selected entry in Data Register 0-3. The entry uses a 116-bit encoding when parity is enabled and a 113-bit encoding when parity is disabled.

Data Register 0[31:0]	TLB Descriptor[31:0].
Data Register 1[31:0]	TLB Descriptor[63:32].
Data Register 2[31:0]	TLB Descriptor[95:64].
Data Register 3[20:0]	TLB Descriptor[115:96].

The following table shows the data fields in the TLB descriptor.

Table C5-8 Main TLB descriptor data fields

Bits	Name	Description
[115:113]	Parity	If CPU cache protection is not implemented, these bits are absent.
[112:111]	S2 Level	The stage 2 level that gave this translation: 0b00 No stage 2 translation performed. 0b01 Level 1. 0b10 Level 2. 0b11 Level 3.

Table C5-8 Main TLB descriptor data fields (continued)

Bits	Name	Description
[110:108]	S1 Size	The stage 1 size that gave this translation. In the VMSAv8-32 Long-descriptor translation table format and the VMSAv8-64 translation table format, domain[2] is used in conjunction with S1 Size, {domain[2], S1 size}: 0b0000 4KB. 0b0001 16KB. 0b0010 64KB. 0b0100 2MB. 0b0110 32MB. 0b0111 512MB. 0b1111 1GB.
[107:104]	Domain	In VMSAv7 format, indicates one of sixteen memory regions. In non-VMSAv7 formats: <ul style="list-style-type: none"> • Domain[0] stores the contiguous bit information. • Domain[1] stores the page size MSB for the combined page size. • Domain[2] stores the page size MSB for the stage 1 page size.
[103:96]	Memory Type and shareability	See <i>TLB encoding for memory types and shareability</i> .
[95]	XS2	Stage2 executable permissions.
[94]	XS1Nonusr	Non user mode executable permissions.
[93]	XS1Usr	User mode executable permissions.
[92-65]	PA	Physical Address.
[64]	NS, descriptor	Security state allocated to memory region.
[63:62]	HAP	Hypervisor access permissions.
[61:59]	AP or HYP	Access permissions from stage-1 translation, or select EL2 or flag.
[58]	nG	Not global.
[57:55]	Size	This field shows the encoding for the combined page size for stage 1 and stage 2. In the VMSAv8-32 Long-descriptor translation table format and the VMSAv8-64 translation table format, domain[1] is used in conjunction with Size, {domain[1], Size}: 0b0001 4KB. 0b1001 16KB. 0b0011 64KB. 0b0101 2MB. 0b1011 32MB. 0b0111 512MB.
[54:39]	ASID	Address Space Identifier.
[38:31]	VMID	Virtual Machine Identifier.
[30]	NS (walk)	Security state that the entry was fetched in.
[29:2]	VA	Virtual Address.

Table C5-8 Main TLB descriptor data fields (continued)

Bits	Name	Description
[1]	Address Sign bit	VA[48] sign bit.
[0]	Valid	Valid bit: 0 Entry does not contain valid data. 1 Entry contains valid data.

The following table shows the main TLB memory types and shareability.

Table C5-9 TLB encoding for memory types and shareability

Bits	Memory type	Description
[7]	Device Non-coherent, Outer WB Non-coherent, Outer NC Non-coherent, Outer WT	0
	Coherent, Inner WB and Outer WB	1
[6]	Device Non-coherent, Outer WB	0
	Non-coherent, Outer NC Non-coherent, Outer WT	1
	Coherent, Inner WB and Outer WB	Transience: 0 Non-transient 1 Transient.

Table C5-9 TLB encoding for memory types and shareability (continued)

Bits	Memory type	Description
[5:4]	Device	Stage 1 (Non-device) overridden by stage 2 (Device) 00 Not overridden 01 Overridden.
	Non-coherent, Outer WB	Inner type: 10 NC. 11 WT.
	Non-coherent, Outer NC	11
	Non-coherent, Outer WT	Inner type: 00 NC. 01 WB. 10 WT.
	Coherent, Inner WB and Outer WB	Inner allocation hint: 00 NA. 01 WA. 10 RA. 11 WRA.
[3:2]	Device	Device type: 00 nGnRnE. 01 nGnRE. 10 nGRE. 11 GRE.
	Non-coherent, Outer WB Non-coherent, Outer WT Coherent, Inner WB and Outer WB	Outer allocation hint: 00 NA. 01 WA. 10 RA. 11 WRA.
	Non-coherent, Outer NC	Inner type: 00 NC. 01 WB. 10 WT. 11 Unused.
	[1:0]	Device Non-coherent, Outer WB Non-coherent, Outer NC Non-coherent, Outer WT Coherent, Inner WB and Outer WB

Related information

C5.5 Encoding for walk cache on page C5-337.

C5.6 Encoding for IPA cache on page C5-338.

C5.1 About direct access to internal memory on page C5-328.

C5.5 Encoding for walk cache

The following table shows the data fields in the walk cache descriptor.

Table C5-10 Walk cache descriptor fields

Bits	Name	Description												
[115:113]	Parity bits	If CPU cache protection is not implemented, these bits are absent.												
[112:83]	PA	Physical Address of the second, last, translation level.												
[82:60]	VA	Virtual address.												
[59]	VA sign	Virtual address sign bit.												
[58:55]	-	Reserved, must be zero.												
[54:39]	ASID	Address Space Identifier.												
[38:31]	VMID	Virtual Machine Identifier.												
[30]	NS, walk	Security state that the entry was fetched in.												
[29:23]	-	Reserved, must be zero.												
[22:19]	Domain	Valid only if the entry was fetched in VMSAv7 format.												
[18:16]	Entry size	Memory size to which entry maps: <table style="margin-left: 20px; border: none;"> <tr> <td>0b100</td> <td>1MB.</td> </tr> <tr> <td>0b101</td> <td>2MB.</td> </tr> <tr> <td>0b010</td> <td>8MB.</td> </tr> <tr> <td>0b110, 0b011</td> <td>32MB.</td> </tr> <tr> <td>0b001</td> <td>128MB.</td> </tr> <tr> <td>0b111</td> <td>512MB.</td> </tr> </table>	0b100	1MB.	0b101	2MB.	0b010	8MB.	0b110, 0b011	32MB.	0b001	128MB.	0b111	512MB.
0b100	1MB.													
0b101	2MB.													
0b010	8MB.													
0b110, 0b011	32MB.													
0b001	128MB.													
0b111	512MB.													
[15]	NSTable	Combined NSTable bits from first and second-level stage 1 tables or NS descriptor (VMSA).												
[14]	PXNTable	Combined PXNTable bits from stage1 descriptors up to last level.												
[13]	XNTable	Combined XNTable bit from stage1 descriptors up to last level.												
[12:11]	APTable	Combined APTable bits from stage1 descriptors up to last level.												
[10]	EL3	Set if the entry was fetched in AArch64 EL3 mode.												
[9]	EL2	Set if the entry was fetched in EL2 mode.												
[8:1]	Attrs	Physical attributes of the final level stage 1 table.												
[0]	Valid	Valid bit: <table style="margin-left: 20px; border: none;"> <tr> <td>0</td> <td>Entry does not contain valid data.</td> </tr> <tr> <td>1</td> <td>Entry contains valid data.</td> </tr> </table>	0	Entry does not contain valid data.	1	Entry contains valid data.								
0	Entry does not contain valid data.													
1	Entry contains valid data.													

C5.6 Encoding for IPA cache

The following table shows the data fields in the IPA cache descriptor.

Table C5-11 IPA cache descriptor fields

Bits	Name	Description
[115:113]	Parity bits	If CPU cache protection is not implemented, these bits are absent.
[112:85]	PA	Physical address.
[84:62]	IPA	Unused lower bits, page size dependent, must be zero.
[61:59]	-	Reserved, must be zero.
[58:55]	Size	Stage 2 page size. The values are: 0b0001 4KB. 0b1001 16KB. 0b0011 64KB. 0b0101 2MB. 0b1011 32MB. 0b0111 512MB.
[54:39]	-	Reserved, must be zero.
[38:31]	VMID	Virtual Machine Identifier.
[30:12]	-	Reserved, must be zero.
[11:10]	Entry granule	The values are: 0b00 4KB. 0b10 16KB. 0b01 64KB.
[9:6]	Memattrs	Memory attributes.
[5]	XN	Execute Never.
[4:3]	HAP	Hypervisor access permissions.
[2:1]	SH	Shareability.
[0]	Valid	The entry contains valid data.

Chapter C6

Debug AArch64 registers

This chapter describes the debug registers in the AArch64 execution state and shows examples of how to use them

It contains the following sections:

- *C6.1 AArch64 debug register summary* on page C6-340.
- *C6.2 Debug Breakpoint Control Registers, EL1* on page C6-342.
- *C6.3 Debug Watchpoint Control Registers, EL1* on page C6-345.
- *C6.4 Debug Claim Tag Set register, EL1* on page C6-347.

C6.1 AArch64 debug register summary

This section summarizes the debug control registers that are accessible in the AArch64 Execution state.

These registers, listed in the following table, are accessed by the MRS and MSR instructions in the order of Op0, CRn, Op1, CRm, Op2.

See [C7.1 Memory-mapped debug register summary on page C7-350](#) for a complete list of registers accessible from the external debug interface. The 64-bit registers cover two addresses on the external memory interface. For those registers not described in this chapter, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

Table C6-1 AArch64 debug register summary

Name	Type	Reset	Width	Description
OSDTRRX_EL1	RW	-	32	Debug Data Transfer Register, Receive, External View
DBGBVR0_EL1	RW	-	64	Debug Breakpoint Value Register 0
DBGBCR0_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
DBGWVR0_EL1	RW	-	64	Debug Watchpoint Value Register 0
DBGWCR0_EL1	RW	-	32	C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345
DBGBVR1_EL1	RW	-	64	Debug Breakpoint Value Register 1
DBGBCR1_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
DBGWVR1_EL1	RW	-	64	Debug Watchpoint Value Register 1
DBGWCR1_EL1	RW	-	32	C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345
MDCCINT_EL1	RW	0x00000000	32	Monitor Debug Comms Channel Interrupt Enable Register
MDSCR_EL1	RW	-	32	B1.63 Monitor Debug System Control Register, EL1 on page B1-240
DBGBVR2_EL1	RW	-	64	Debug Breakpoint Value Register 2
DBGBCR2_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
DBGWVR2_EL1	RW	-	64	Debug Watchpoint Value Register 2
DBGWCR2_EL1	RW	-	32	C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345
OSDTRTX_EL1	RW	-	32	Debug Data Transfer Register, Transmit, External View
DBGBVR3_EL1	RW	-	64	Debug Breakpoint Value Register 3
DBGBCR3_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
DBGWVR3_EL1	RW	-	64	Debug Watchpoint Value Register 3
DBGWCR3_EL1	RW	-	32	C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345
DBGBVR4_EL1	RW	-	64	Debug Breakpoint Value Register 4

Table C6-1 AArch64 debug register summary (continued)

Name	Type	Reset	Width	Description
DBGBCR4_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
DBGBVR5_EL1	RW	-	64	Debug Breakpoint Value Register 5
DBGBCR5_EL1	RW	-	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
OSECCR_EL1	RW	-	32	Debug OS Lock Exception Catch Register
MDCCSR_EL0	RO	-	32	Monitor Debug Comms Channel Status Register
DBGDTR_EL0	RW	-	64	Debug Data Transfer Register, half-duplex
DBGDTRTX_EL0	WO	-	32	Debug Data Transfer Register, Transmit, Internal View
DBGDTRRX_EL0	RO	-	32	Debug Data Transfer Register, Receive, Internal View
MDRAR_EL1	RO	Resets to the physical address of the ROM table +3.	64	Debug ROM Address Register
OSLAR_EL1	WO	-	32	Debug OS Lock Access Register
OSLSR_EL1	RO	0x0000000A	32	Debug OS Lock Status Register
OSDLR_EL1	RW	0x00000000	32	Debug OS Double Lock Register
DBGPRCR_EL1	RW	-	32	Debug Power/Reset Control Register
DBGCLAIMSET_EL1	RW	0x000000FF	32	Debug Claim Tag Set Register
DBGCLAIMCLR_EL1	RW	0x00000000	32	Debug Claim Tag Clear Register
DBGAUTHSTATUS_EL1	RO	-	32	Debug Authentication Status Register

C6.2 Debug Breakpoint Control Registers, EL1

The DBGBCR_n_EL1 characteristics are:

Purpose

Holds control information for a breakpoint. Each DBGBVR_EL1 is associated with a DBGBCR_EL1 to form a *Breakpoint Register Pair* (BRP). DBGBVR_n_EL1 is associated with DBGBCR_n_EL1 to form BRP_n.

The range of *n* for DBGBCR_n_EL1 is 0 to 5.

Usage constraints

These registers are accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

DBGBCR_n_EL1 are architecturally mapped to the external DBGBCR_n_EL1 registers.

Attributes

See [C6.1 AArch64 debug register summary on page C6-340](#).

The debug logic reset value of a DBGBCR_n_EL1 is UNKNOWN.

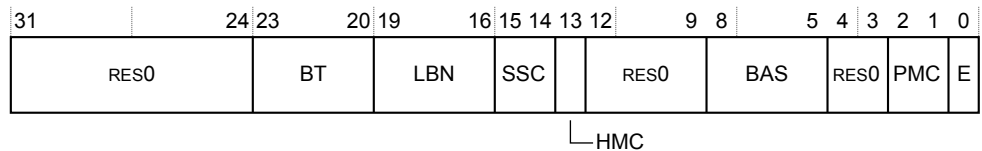


Figure C6-1 DBGBCR_n_EL1

[31:24]

Reserved, RES0.

BT, [23:20]

Breakpoint Type. This field controls the behavior of Breakpoint debug event generation. This includes the meaning of the value held in the associated DBGBVR_n_EL1, indicating whether it is an instruction address match or mismatch or a Context match. It also controls whether the breakpoint is linked to another breakpoint. The possible values are:

- 0b0000 Unlinked instruction address match.
- 0b0001 Linked instruction address match.
- 0b0010 Unlinked Context ID match.
- 0b0011 Linked Context ID match.
- 0b0100 Unlinked instruction address mismatch.
- 0b0101 Linked instruction address mismatch.
- 0b1000 Unlinked VMID match.
- 0b1001 Linked VMID match.
- 0b1010 Unlinked VMID + Context ID match.
- 0b1011 Linked VMID + Context ID match.

All other values are reserved.

The field break down is:

- BT[3:1]: Base type. If the breakpoint is not context-aware, these bits are RES0. Otherwise, the possible values are:

- 0b000 Match address. $DBGBVRn_EL1$ is the address of an instruction.
- 0b001 Match context ID. $DBGBVRn_EL1[31:0]$ is a context ID.
- 0b010 Address mismatch. Mismatch address. Behaves as type 0b000 if either:
 - In an AArch64 translation regime.
 - Halting debug-mode is enabled and halting is allowed.Otherwise, $DBGBVRn_EL1$ is the address of an instruction to be stepped.
- 0b100 Match VMID. $DBGBVRn_EL1[39:32]$ is a VMID.
- 0b101 Match VMID and context ID. $DBGBVRn_EL1[31:0]$ is a context ID, and $DBGBVRn_EL1[39:32]$ is a VMID.

- BT[0]: Enable linking.

LBN, [19:16]

Linked breakpoint number. For Linked address matching breakpoints, this specifies the index of the Context-matching breakpoint linked to.

SSC, [15:14]

Security State Control. Determines the security states that a breakpoint debug event for breakpoint n is generated.

This field must be interpreted with the *Higher Mode Control (HMC)*, and *Privileged Mode Control (PMC)*, fields to determine the mode and security states that can be tested.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for possible values of the fields.

HMC, [13]

Hyp Mode Control bit. Determines the debug perspective for deciding when a breakpoint debug event for breakpoint n is generated.

This bit must be interpreted with the SSC and PMC fields to determine the mode and security states that can be tested.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for possible values of the fields.

[12:9]

Reserved, RES0.

BAS, [8:5]

Reserved, RES1

[4:3]

Reserved, RES0.

PMC, [2:1]

Privileged Mode Control. Determines the exception level or levels that a breakpoint debug event for breakpoint n is generated.

This field must be interpreted with the SSC and HMC fields to determine the mode and security states that can be tested.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for possible values of the fields.

Bits[2:1] have no effect for accesses made in Hyp mode.

E, [0]

Enable breakpoint. This bit enables the BRP:

- 0 BRP disabled.
- 1 BRP enabled.

A BRP never generates a breakpoint debug event when it is disabled.

The value of `DBGBCRn_EL1.E` is UNKNOWN on reset. A debugger must ensure that `DBGBCRn_EL1.E` has a defined value before it enables debug.

To access the `DBGBCRn_EL1`, read or write the register with:

```
MRS <Xt>, DBGBCRn_EL1; Read Debug Breakpoint Control Register n  
MSR DBGBCRn_EL1, <Xt>; Write Debug Breakpoint Control Register n
```

The `DBGBCRn_EL1` can be accessed through the external debug interface, offset `0x4n8`. The range of bits for `DBGBCRn_EL1` is 0 to 5.

C6.3 Debug Watchpoint Control Registers, EL1

The $DBGWCR_n_EL1$ characteristics are:

Purpose

Holds control information for a watchpoint. Each $DBGWCR_EL1$ is associated with a $DBGWVR_EL1$ to form a *Watchpoint Register Pair* (WRP). $DBGWCR_n_EL1$ is associated with $DBGWVR_n_EL1$ to form WRP_n .

The range of n for $DBGWCR_n_EL1$ is 0 to 3.

Usage constraints

These registers are accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

The $DBGWCR_n_EL1$ are architecturally mapped to the external $DBGWCR_n_EL1$ registers.

Attributes

See [C6.1 AArch64 debug register summary on page C6-340](#).

The debug logic reset value of a $DBGWCR_EL1$ is UNKNOWN.

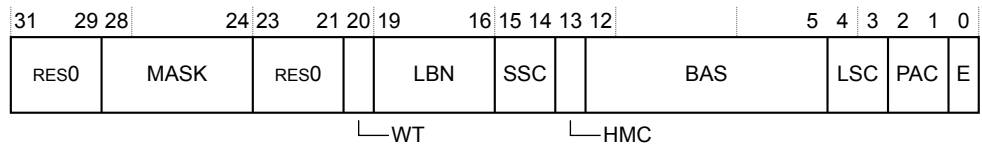


Figure C6-2 $DBGWCR_EL1$

[31:29]

Reserved, RES0.

MASK, [28:24]

Address mask. Only objects up to 2GB can be watched using a single mask.

- 0b0000 No mask
- 0b0001 Reserved
- 0b0010 Reserved

Other values mask the corresponding number of address bits, from 0b00011 masking 3 address bits (0x00000007 mask for address) to 0b11111 masking 31 address bits (0x7FFFFFFF mask for address).

[23:21]

Reserved, RES0.

WT, [20]

Watchpoint type. Possible values are:

- 0 Unlinked data address match.
- 1 Linked data address match.

On Cold reset, the field reset value is architecturally UNKNOWN.

LBN, [19:16]

Linked breakpoint number. For Linked data address watchpoints, this specifies the index of the Context-matching breakpoint linked to.

On Cold reset, the field reset value is architecturally UNKNOWN.

SSC, [15:14]

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.

On Cold reset, the field reset value is architecturally UNKNOWN.

HMC, [13]

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.

On Cold reset, the field reset value is architecturally UNKNOWN.

BAS, [12:5]

Byte address select. Each bit of this field selects whether a byte from within the word or double-word addressed by `DBGWVR n _EL1` is being watched. See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

LSC, [4:3]

Load/store access control. This field enables watchpoint matching on the type of access being made. The possible values are:

- `0b01` Match instructions that load from a watchpointed address.
- `0b10` Match instructions that store to a watchpointed address.
- `0b11` 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.

Ignored if E is 0.

On Cold reset, the field reset value is architecturally UNKNOWN.

PAC, [2:1]

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.

On Cold reset, the field reset value is architecturally UNKNOWN.

E, [0]

Enable watchpoint n . Possible values are:

- `0` Watchpoint disabled.
- `1` Watchpoint enabled.

On Cold reset, the field reset value is architecturally UNKNOWN.

To access the `DBGWCR n _EL1`:

```
MRS <Xt>, DBGWCR $n$ _EL1; Read Debug Watchpoint Control Register  $n$   
MSR DBGWCR $n$ _EL1, <Xt>; Write Debug Watchpoint Control Register  $n$ 
```

The `DBGWCR n _EL1` can be accessed through the external debug interface, offset `0x8n8`. The range of n for `DBGWCR n _EL1` is 0 to 3.

C6.4 Debug Claim Tag Set register, EL1

The DBGCLAIMSET_EL1 characteristics are:

Purpose

Used by software to set CLAIM bits to 1.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
-	RW	RW	RW	RW	RW

Configurations

DBGCLAIMSET_EL1 is architecturally mapped to the external register
 DBGCLAIMSET_EL1.

Attributes

DBGCLAIMSET_EL1 is a 32-bit register.



Figure C6-3 DBGCLAIMSET_EL1 bit assignments

[31:8]

Reserved, RES0.

CLAIM, [7:0]

Claim set bits.

Writing a 1 to one of these bits sets the corresponding CLAIM bit to 1. This is an indirect write to the CLAIM bits.

A single write operation can set multiple bits to 1. Writing 0 to one of these bits has no effect.

To access the DBGCLAIMSET_EL1 in AArch64 Execution state, read or write the register with:

```
MRS <Xt>, DBGCLAIMSET_EL1 ; Read DBGCLAIMSET_EL1 into XtMSR DBGCLAIMSET_EL1, <Xt> ; Write Xt to DBGCLAIMSET_EL1
```

The DBGCLAIMSET_EL1 can be accessed through the internal memory-mapped interface and the external debug interface, offset 0xFA0.

Chapter C7

Debug memory mapped registers

This chapter describes the debug memory-mapped registers and shows examples of how to use them.

It contains the following sections:

- *C7.1 Memory-mapped debug register summary* on page C7-350.
- *C7.2 External Debug Reserve Control Register* on page C7-354.
- *C7.3 External Debug Integration Mode Control Register* on page C7-355.
- *C7.4 External Debug Device ID Register 0* on page C7-356.
- *C7.5 External Debug Device ID Register 1* on page C7-357.
- *C7.6 External Debug Processor Feature Register* on page C7-358.
- *C7.7 External Debug Feature Register* on page C7-360.
- *C7.8 External Debug Peripheral Identification Registers* on page C7-362.
- *C7.9 External Debug Peripheral Identification Register 0* on page C7-363.
- *C7.10 External Debug Peripheral Identification Register 1* on page C7-364.
- *C7.11 External Debug Peripheral Identification Register 2* on page C7-365.
- *C7.12 External Debug Peripheral Identification Register 3* on page C7-366.
- *C7.13 External Debug Peripheral Identification Register 4* on page C7-367.
- *C7.14 External Debug Peripheral Identification Register 5-7* on page C7-368.
- *C7.15 External Debug Component Identification Registers* on page C7-369.
- *C7.16 External Debug Component Identification Register 0* on page C7-370.
- *C7.17 External Debug Component Identification Register 1* on page C7-371.
- *C7.18 External Debug Component Identification Register 2* on page C7-372.
- *C7.19 External Debug Component Identification Register 3* on page C7-373.

C7.1 Memory-mapped debug register summary

The following table shows the offset address for the registers that are accessible from the external debug interface.

For those registers not described in this chapter, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

Table C7-1 Memory-mapped debug register summary

Offset	Name	Type	Width	Description
0x000-0x01C	-	-		Reserved
0x020	EDESR	RW	32	External Debug Event Status Register
0x024	EDECR	RW	32	External Debug Execution Control Register
0x028-0x02C	-	-	-	Reserved
0x030	EDWAR[31:0]	RO	64	External Debug Watchpoint Address Register
0x034	EDWAR[63:32]			
0x038-0x07C	-	-	-	Reserved
0x080	DBGDTRRX_EL0	RW	32	Debug Data Transfer Register, Receive
0x084	EDITR	WO	32	External Debug Instruction Transfer Register
0x088	EDSCR	RW	32	External Debug Status and Control Register
0x08C	DBGDTRTX_EL0	RW	32	Debug Data Transfer Register, Transmit
0x090	EDRCR	WO	32	C7.2 External Debug Reserve Control Register on page C7-354
0x094	EDACR	RW	32	External Debug Auxiliary Control Register
0x098	EDECCR	RW	32	External Debug Exception Catch Control Register
0x09C	-	-	32	Reserved
0x0A0	EDPCSRlo	RO	32	External Debug Program Counter Sample Register, low word
0x0A4	EDCIDSR	RO	32	External Debug Context ID Sample Register
0x0A8	EDVIDSR	RO	32	External Debug Virtual Context Sample Register
0x0AC	EDPCSRhi	RO	32	External Debug Program Counter Sample Register, high word
0x0B0-0x2FC	-	-	-	Reserved
0x300	OSLAR_EL1	WO	32	OS Lock Access Register
0x304-0x30C	-	-	-	Reserved
0x310	EDPRCR	RW	32	External Debug Power/Reset Control Register
0x314	EDPRSR	RO	32	External Debug Processor Status Register
0x318-0x3FC	-	-	--	Reserved
0x400	DBGBVR0_EL1[31:0]	RW	64	Debug Breakpoint Value Register 0
0x404	DBGBVR0_EL1[63:32]			
0x408	DBGBCR0_EL1	RW	32	C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342
0x40C	-	-	-	Reserved

Table C7-1 Memory-mapped debug register summary (continued)

Offset	Name	Type	Width	Description
0x410	DBGBVR1_EL1[31:0]	RW	64	Debug Breakpoint Value Register 1
0x414	DBGBVR1_EL1[63:32]			
0x418	DBGBCR1_EL1	RW	32	<i>C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342</i>
0x41C	-	-	-	Reserved
0x420	DBGBVR2_EL1[31:0]	RW	64	Debug Breakpoint Value Register 2
0x424	DBGBVR2_EL1[63:32]			
0x428	DBGBCR2_EL1	RW	32	<i>C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342</i>
0x42C	-	-	-	Reserved
0x430	DBGBVR3_EL1[31:0]	RW	64	Debug Breakpoint Value Register 3
0x434	DBGBVR3_EL1[63:32]			
0x438	DBGBCR3_EL1	RW	32	<i>C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342</i>
0x43C	-	-	-	Reserved
0x440	DBGBVR4_EL1[31:0]	RW	64	Debug Breakpoint Value Register 4
0x444	DBGBVR4_EL1[63:32]			
0x448	DBGBCR4_EL1	RW	32	<i>C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342</i>
0x44C	-	-	-	Reserved
0x450	DBGBVR5_EL1[31:0]	RW	64	Debug Breakpoint Value Register 5
0x454	DBGBVR5_EL1[63:32]			
0x458	DBGBCR5_EL1	RW	32	<i>C6.2 Debug Breakpoint Control Registers, EL1 on page C6-342</i>
0x45C-0x7FC	-	-	-	Reserved
0x800	DBGWVR0_EL1[31:0]	RW	64	Debug Watchpoint Value Register 0
0x804	DBGWVR0_EL1[63:32]			
0x808	DBGWCR0_EL1	RW	32	<i>C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345</i>
0x80C	-	-	-	Reserved
0x810	DBGWVR1_EL1[31:0]	RW	64	Debug Watchpoint Value Register 1
0x814	DBGWVR1_EL1[63:32]			
0x818	DBGWCR1_EL1	RW	32	<i>C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345</i>
0x81C	-	-	-	Reserved
0x820	DBGWVR2_EL1[31:0]	RW	64	Debug Watchpoint Value Register 2
0x824	DBGWVR2_EL1[63:32]			
0x828	DBGWCR2_EL1	RW	32	<i>C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345</i>
0x82C	-	-	-	Reserved
0x830	DBGWVR3_EL1[31:0]	RW	64	Debug Watchpoint Value Register 0,
0x834	DBGWVR3_EL1[63:32]			
0x838	DBGWCR3_EL1	RW	32	<i>C6.3 Debug Watchpoint Control Registers, EL1 on page C6-345</i>

Table C7-1 Memory-mapped debug register summary (continued)

Offset	Name	Type	Width	Description
0x83C-0xCFC	-	-	-	Reserved
0xD00	MIDR_EL1	RO	32	<i>B1.64 Main ID Register, EL1 on page B1-243</i>
0xD04-0xD1C	-	-	-	Reserved
0xD20	EDPFR[31:0]	RO	64	<i>C7.6 External Debug Processor Feature Register on page C7-358</i>
0xD24	EDPFR[63:32]			
0xD28	EDDFR[31:0]	RO	64	<i>C7.7 External Debug Feature Register on page C7-360</i>
0xD2C	EDDFR[63:32]			
0xD30-0xD34	-	-	-	Reserved
0xD38-0xD3C	-	-	-	Reserved
0xD60-0xEFC	-	-	-	Reserved
0xF00	EDITCTRL	RW	32	<i>C7.3 External Debug Integration Mode Control Register on page C7-355</i>
0xF04-0xF9C	-	-	-	Reserved
0xFA0	DBGCLAIMSET_EL1	RW	32	Debug Claim Tag Set register
0xFA4	DBGCLAIMCLR_EL1	RW	32	Debug Claim Tag Clear Register
0xFA8	EDDEVAFF0	RO	32	<i>B1.65 Multiprocessor Affinity Register, EL1 on page B1-245</i>
0xFAC	EDDEVAFF1	RO	32	<i>B1.65 Multiprocessor Affinity Register, EL1 on page B1-245</i>
0xFB0	EDLAR	WO	32	External Debug Lock Access Register
0xFB4	EDLSR	RO	32	External Debug Lock Status Register
0xFB8	DBGAUTHSTATUS_EL1	RO	32	Debug Authentication Status Register
0xFBC	EDDEVARCH	RO	32	External Debug Device Architecture Register
0xFC0	EDDEVID2	RO	32	External Debug Device ID Register 2, RES0
0xFC4	EDDEVID1	RO	32	<i>C7.5 External Debug Device ID Register 1 on page C7-357</i>
0xFC8	EDDEVID	RO	32	<i>C7.4 External Debug Device ID Register 0 on page C7-356</i>
0xFCC	EDDEVTYPE	RO	32	External Debug Device Type Register
0xFD0	EDPIDR4	RO	32	<i>C7.13 External Debug Peripheral Identification Register 4 on page C7-367</i>
0xFD4-0xFDC	EDPIDR5-7	RO	32	<i>C7.14 External Debug Peripheral Identification Register 5-7 on page C7-368</i>
0xFE0	EDPIDR0	RO	32	<i>C7.9 External Debug Peripheral Identification Register 0 on page C7-363</i>
0xFE4	EDPIDR1	RO	32	<i>C7.10 External Debug Peripheral Identification Register 1 on page C7-364</i>
0xFE8	EDPIDR2	RO	32	<i>C7.11 External Debug Peripheral Identification Register 2 on page C7-365</i>
0xFEC	EDPIDR3	RO	32	<i>C7.12 External Debug Peripheral Identification Register 3 on page C7-366</i>

Table C7-1 Memory-mapped debug register summary (continued)

Offset	Name	Type	Width	Description
0xFF0	EDCIDR0	RO	32	<i>C7.16 External Debug Component Identification Register 0 on page C7-370</i>
0xFF4	EDCIDR1	RO	32	<i>C7.17 External Debug Component Identification Register 1 on page C7-371</i>
0xFF8	EDCIDR2	RO	32	<i>C7.18 External Debug Component Identification Register 2 on page C7-372</i>
0xFFC	EDCIDR3	RO	32	<i>C7.19 External Debug Component Identification Register 3 on page C7-373</i>

C7.2 External Debug Reserve Control Register

The EDRCR characteristics are:

Purpose

This register is used to allow imprecise entry to Debug state and clear sticky bits in EDSCR.

This register is part of the Debug registers functional group.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	SLK	Default
Error	Error	Error	WI	WO

Configurations

EDRCR is in the Core power domain.

Attributes

See [C7.1 Memory-mapped debug register summary](#) on page C7-350.

EDRCR is a 32-bit register.

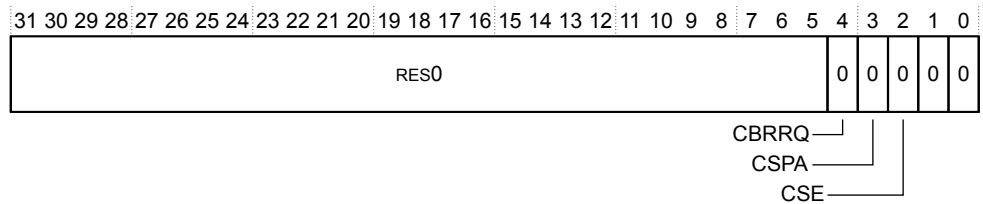


Figure C7-1 EDRCR bit assignments

[31:5]

Reserved, RES0.

CBRRQ, [4]

Allow imprecise entry to Debug state. The actions on writing to this bit are:

- 0 No action.
- 1 Allow imprecise entry to Debug state, for example by canceling pending bus accesses. 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.

CSPA, [3]

Clear Sticky Pipeline Advance. This bit is used to clear the EDSCR.PipeAdv bit to 0. The actions on writing to this bit are:

- 0 No action.
- 1 Clear the EDSCR.PipeAdv bit to 0.

CSE, [2]

Clear Sticky Error. Used to clear the EDSCR cumulative error bits to 0. The actions on writing to this bit are:

- 0 No action
- 1 Clear the EDSCR.{TXU, RXO, ERR} bits, and, if the processor is in Debug state, the EDSCR.ITO bit, to 0.

[1:0]

Reserved, RES0.

The EDRCR can be accessed through the external debug interface, offset 0x090.

C7.3 External Debug Integration Mode Control Register

The EDITCTRL characteristics are:

Purpose

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 processor, for integration testing or topology detection.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	RO	RW

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

EDITCTRL is in the processor power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

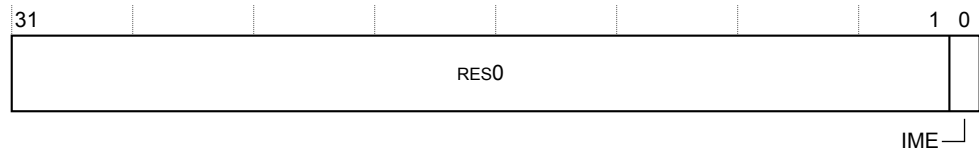


Figure C7-2 EDITCTRL bit assignments

[31:1]

Reserved, RES0.

IME, [0]

Integration Mode Enable.

RES0. The device does not revert to an integration mode to enable integration testing or topology detection.

The EDITCTRL can be accessed through the external debug interface, offset 0xF00.

C7.4 External Debug Device ID Register 0

The EDDEVID characteristics are:

Purpose

Provides extra information for external debuggers about features of the debug implementation.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDDEVID is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

31	28 27	24 23	4	3	0
RES0	AuxRegs	RES0			PC Sample

Figure C7-3 EDDEVID bit assignments

[31:28]

Reserved, RES0.

AuxRegs, [27:24]

Indicates support for Auxiliary registers:

0x0 None supported.

[23:4]

Reserved, RES0.

PC Sample, [3:0]

Indicates the level of sample-based profiling support using external debug registers 40 to 43:

0x3 EDPCSR, EDCIDSR, and EDVIDSR are implemented.

The EDDEVID can be accessed through the external debug interface, offset 0xFC8.

C7.5 External Debug Device ID Register 1

The EDDEVID1 characteristics are:

Purpose

Provides extra information for external debuggers about features of the debug implementation.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDDEVID1 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

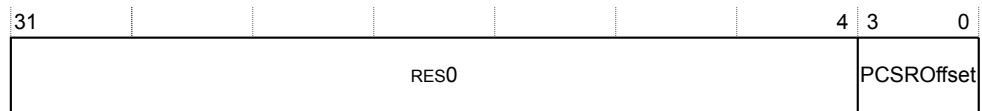


Figure C7-4 EDDEVID1 bit assignments

[31:4]

Reserved, RES0.

PCSROffset, [3:0]

Indicates the offset applied to PC samples returned by reads of EDPCSR:

0x2 EDPCSR samples have no offset applied.

The EDDEVID1 can be accessed through the external debug interface, offset 0xFC4.

C7.6 External Debug Processor Feature Register

The EDPFR characteristics are:

Purpose

Provides additional information about implemented PE features in AArch64.

Usage constraints

This register is accessible as follows:

Default
RO

Configurations

The EDPFR is:

- Architecturally mapped to the AArch64 ID_AA64PFR0_EL1 register. See [B1.51 AArch64 Processor Feature Register 0, EL1](#) on page B1-217.
- EDPFR is in the Debug power domain.

Attributes

EDPFR is a 64-bit register.

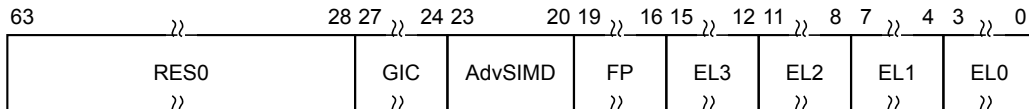


Figure C7-5 EDPFR bit assignments

[63:28]

Reserved, RES0.

GIC, [27:24]

System register GIC interface. Defined values are:

- 0x0 No System register interface to the GIC is supported.
- 0x1 System register interface to the GIC CPU interface is supported.

All other values are reserved.

AdvSIMD, [23:20]

Advanced SIMD. Defined values are:

- 0x0 Advanced SIMD is implemented.
- 0xF Advanced SIMD is not implemented.

All other values are reserved.

FP, [19:16]

Floating-point. Defined values are:

- 0x0 Floating-point is implemented.
- 0xF Floating-point is not implemented.

All other values are reserved.

EL3 handling, [15:12]

EL3 exception handling:

- 0x1 Instructions can be executed at EL3 in AArch64 state.

EL2 handling, [11:8]

EL2 exception handling:

0x1 Instructions can be executed at EL2 in AArch64 state.

EL1 handling, [7:4]

EL1 exception handling. The possible values are:

0x1 Instructions can be executed at EL1 in AArch64 state.

EL0 handling, [3:0]

EL0 exception handling. The possible values are:

0x1 Instructions can be executed at EL0 in AArch64 state.

The EDPFR[31:0] can be accessed through the external debug interface, offset 0xD20.

The EDPFR[63:32] can be accessed through the external debug interface, offset 0xD24.

C7.7 External Debug Feature Register

The EDDFR characteristics are:

Purpose

Provides top level information about the debug system in AArch64.

Usage constraints

This register is accessible as follows:

Default
RO

Configurations

External register EDDFR is architecturally mapped to the AArch64 ID_AA64DFR0_EL1 register. See [B1.49 AArch64 Debug Feature Register 0, EL1](#) on page B1-213.

EDDFR is in the Debug power domain.

Attributes

EDDFR is a 64-bit register.

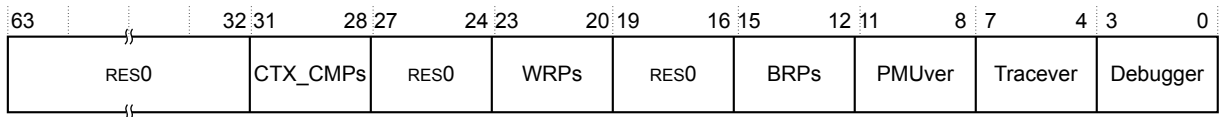


Figure C7-6 EDDFR bit assignments

[63:32]

Reserved, RES0.

CTX_CMPs, [31:28]

Number of breakpoints that are context-aware, minus 1. These are the highest numbered breakpoints.

[27:24]

Reserved, RES0.

WRPs, [23:20]

Number of watchpoints, minus 1. The value of 0b0000 is reserved.

[19:16]

Reserved, RES0.

BRPs, [15:12]

Number of breakpoints, minus 1. The value of 0b0000 is reserved.

PMUVer, [11:8]

Performance Monitors extension version. Indicates whether system register interface to Performance Monitors extension is implemented. Defined values are:

0x0000 Performance Monitors extension system registers not implemented.

0x0001 Performance Monitors extension system registers implemented, PMUv3.

0x1111 IMPLEMENTATION DEFINED form of performance monitors supported, PMUv3 not supported.

All other values are reserved.

TraceVer [7:4]

Trace support. Indicates whether system register interface to a trace macrocell is implemented. Defined values are:

0x0000 Trace macrocell system registers not implemented.

0x0001 Trace macrocell system registers implemented.

All other values are reserved.

A value of 0x0000 only indicates that no system register interface to a trace macrocell is implemented. A trace macrocell might nevertheless be implemented without a system register interface.

UNKNOWN, [7:4]

Reserved, UNKNOWN.

EDDFR[31:0] can be accessed through the external debug interface, offset 0xD28.

EDDFR[63:32] can be accessed through the external debug interface, offset 0xD2C.

C7.8 External Debug Peripheral Identification Registers

The External Debug Peripheral Identification Registers provide standard information required for all components that conform to the ARM Debug Interface v5 specification.

The following table lists the External Debug Peripheral Identification Registers.

Table C7-2 Summary of the External Debug Peripheral Identification Registers

Register	Value	Offset
Peripheral ID4	0x04	0xFD0
Peripheral ID5	0x00	0xFD4
Peripheral ID6	0x00	0xFD8
Peripheral ID7	0x00	0xFDC
Peripheral ID0	0x12	0xFE0
Peripheral ID1	0xBD	0xFE4
Peripheral ID2	0x1B	0xFE8
Peripheral ID3	0x00	0xFEC

Only bits[7:0] of each Peripheral ID Register are used, with bits[31:8] reserved. Together, the eight Peripheral ID Registers define a single 64-bit Peripheral ID.

C7.9 External Debug Peripheral Identification Register 0

The EDPIDR0 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDPIDR0 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

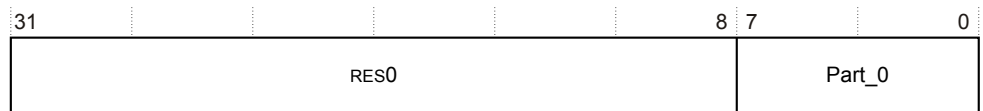


Figure C7-7 EDPIDR0 bit assignments

[31:8]

Reserved, RES0.

Part_0, [7:0]

0x02 Least significant byte of the debug part number.

The EDPIDR0 can be accessed through the external debug interface, offset 0xFE0.

C7.10 External Debug Peripheral Identification Register 1

The EDPIDR1 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDPIDR1 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

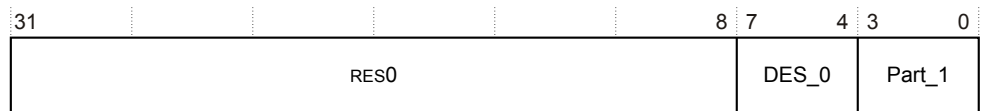


Figure C7-8 EDPIDR1 bit assignments

[31:8]

Reserved, RES0.

DES_0, [7:4]

0xB ARM Limited. This is the least significant nibble of JEP106 ID code.

Part_1, [3:0]

0xD Most significant nibble of the debug part number.

The EDPIDR1 can be accessed through the external debug interface, offset 0xFE4.

C7.11 External Debug Peripheral Identification Register 2

The EDPIDR2 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDPIDR2 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

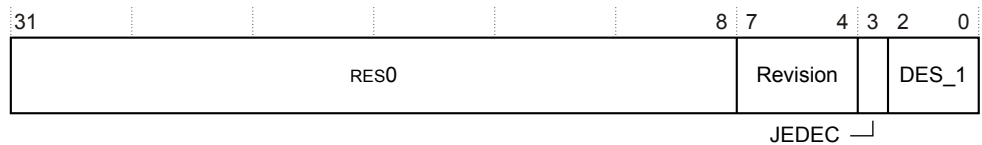


Figure C7-9 EDPIDR2 bit assignments

[31:8]

Reserved, RES0.

Revision, [7:4]

0x1 r0p1.

JEDEC, [3]

0b1 RAO. Indicates a JEP106 identity code is used.

DES_1, [2:0]

0b011 ARM Limited. This is the most significant nibble of JEP106 ID code.

The EDPIDR2 can be accessed through the external debug interface, offset 0xFE8.

C7.12 External Debug Peripheral Identification Register 3

The EDPIDR3 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDPIDR3 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

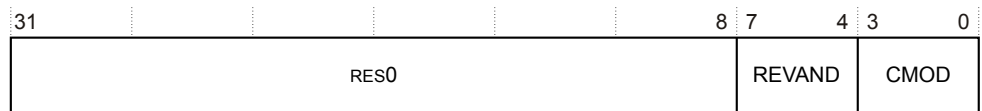


Figure C7-10 EDPIDR3 bit assignments

[31:8]

Reserved, RES0.

REVAND, [7:4]

0x0 Part minor revision.

CMOD, [3:0]

0x0 Customer modified.

The EDPIDR3 can be accessed through the external debug interface, offset 0xFEC.

C7.13 External Debug Peripheral Identification Register 4

The EDPIDR4 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDPIDR4 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

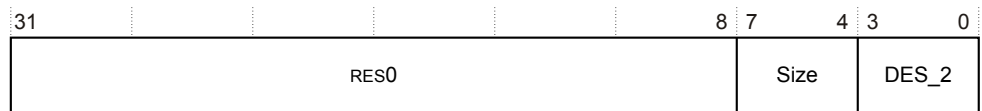


Figure C7-11 EDPIDR4 bit assignments

[31:8]

Reserved, RES0.

Size, [7:4]

0x0 Size of the component. \log_2 the number of 4KB pages from the start of the component to the end of the component ID registers.

DES_2, [3:0]

0x4 ARM Limited. This is the least significant nibble JEP106 continuation code.

The EDPIDR4 can be accessed through the external debug interface, offset 0xFD0.

C7.14 External Debug Peripheral Identification Register 5-7

No information is held in the Peripheral ID5, Peripheral ID6, and Peripheral ID7 Registers. They are reserved for future use and are RES0.

C7.15 External Debug Component Identification Registers

There are four read-only External Debug Component Identification Registers, Component ID0 through Component ID3.

Table C7-3 Summary of the External Debug Component Identification Registers

Register	Value	Offset
Component ID0	0x0D	0xFF0
Component ID1	0x90	0xFF4
Component ID2	0x05	0xFF8
Component ID3	0xB1	0xFFC

The External Debug Component Identification Registers identify Debug as an ARM Debug Interface v5 component.

C7.16 External Debug Component Identification Register 0

The EDCIDR0 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDCIDR0 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

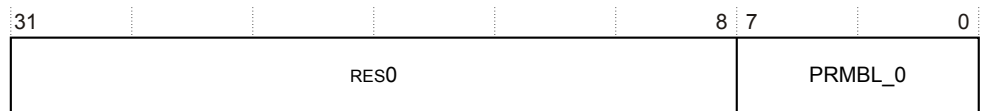


Figure C7-12 EDCIDR0 bit assignments

[31:8]

Reserved, RES0.

PRMBL_0, [7:0]

0x0D Preamble byte 0.

The EDCIDR0 can be accessed through the external debug interface, offset 0xFF0.

C7.17 External Debug Component Identification Register 1

The EDCIDR1 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDCIDR1 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.



Figure C7-13 EDCIDR1 bit assignments

[31:8]

Reserved, RES0.

CLASS, [7:4]

0x9 Debug component.

PRMBL_1, [3:0]

0x0 Preamble.

The EDCIDR1 can be accessed through the external debug interface, offset 0xFF4.

C7.18 External Debug Component Identification Register 2

The EDCIDR2 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDCIDR2 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.

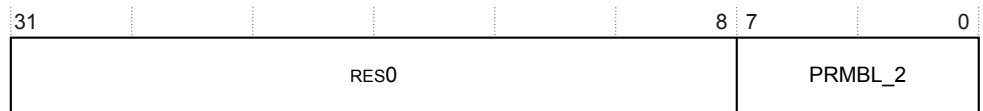


Figure C7-14 EDCIDR2 bit assignments

[31:8]

Reserved, RES0.

PRMBL_2, [7:0]

0x05 Preamble byte 2.

The EDCIDR2 can be accessed through the external debug interface, offset 0xFF8.

C7.19 External Debug Component Identification Register 3

The EDCIDR3 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

Table C1-1 Conditions on external register access to debug registers on page C1-299 describes the condition codes.

Configurations

The EDCIDR3 is in the Debug power domain.

Attributes

See *C7.1 Memory-mapped debug register summary on page C7-350*.



Figure C7-15 EDCIDR3 bit assignments

[31:8]

Reserved, RES0.

PRMBL_3, [7:0]

0xB1 Preamble byte 3.

The EDCIDR3 can be accessed through the external debug interface, offset 0xFFC.

Chapter C8

ROM table

This section describes the ROM table that the debuggers can use to determine which components are implemented. It also describes the ROM table registers.

It contains the following sections:

- *C8.1 About the ROM table* on page C8-376.
- *C8.2 ROM table register interface* on page C8-377.
- *C8.3 ROM table register summary* on page C8-378.
- *C8.4 ROM entry registers* on page C8-379.
- *C8.5 ROM Table Peripheral Identification Registers* on page C8-382.
- *C8.6 ROM Table Peripheral Identification Register 0* on page C8-383.
- *C8.7 ROM Table Peripheral Identification Register 1* on page C8-384.
- *C8.8 ROM Table Peripheral Identification Register 2* on page C8-385.
- *C8.9 ROM Table Peripheral Identification Register 3* on page C8-386.
- *C8.10 ROM Table Peripheral Identification Register 4* on page C8-387.
- *C8.11 ROM Table Peripheral Identification Register 5-7* on page C8-388.
- *C8.12 ROM Table Component Identification Registers* on page C8-389.
- *C8.13 ROM Table Component Identification Register 0* on page C8-390.
- *C8.14 ROM Table Component Identification Register 1* on page C8-391.
- *C8.15 ROM Table Component Identification Register 2* on page C8-392.
- *C8.16 ROM Table Component Identification Register 3* on page C8-393.

C8.1 About the ROM table

The processor includes a ROM table that complies with the ARM CoreSight Architecture Specification.

This table contains a list of components such as processor debug units, processor *Cross Trigger Interfaces* (CTIs), processor *Performance Monitoring Units* (PMUs), and processor *Embedded Trace Macrocell* (ETM) trace units. Debuggers can use the ROM table to determine which components are implemented inside the Cortex-A34 processor.

If a component is not included in your configuration of the Cortex-A34 processor, the corresponding debug APB ROM table entry is still present but the component is marked as not present.

C8.2 ROM table register interface

The interface to the ROM table entries is the APB slave port.

See [C1.2 Debug access](#) on page C1-297.

C8.3 ROM table register summary

The following table shows the offsets from the physical base address of the ROM table.

Table C8-1 ROM table registers

Offset	Name	Type	Description
0x000	ROENTRY0	RO	<i>C8.4 ROM entry registers on page C8-379</i>
0x004	ROENTRY1	RO	
0x008	ROENTRY2	RO	
0x00C	ROENTRY3	RO	
0x010	ROENTRY4	RO	
0x014	ROENTRY5	RO	
0x018	ROENTRY6	RO	
0x01C	ROENTRY7	RO	
0x020	ROENTRY8	RO	
0x024	ROENTRY9	RO	
0x028	ROENTRY10	RO	
0x02C	ROENTRY11	RO	
0x030	ROENTRY12	RO	
0x034	ROENTRY13	RO	
0x038	ROENTRY14	RO	
0x03C	ROENTRY15	RO	
0x040-0xFCC	-	RO	Reserved, RES0
0xFD0	ROMPIDR4	RO	<i>C8.10 ROM Table Peripheral Identification Register 4 on page C8-387</i>
0xFD4	ROMPIDR5	RO	<i>C8.11 ROM Table Peripheral Identification Register 5-7 on page C8-388</i>
0xFD8	ROMPIDR6	RO	
0xFDC	ROMPIDR7	RO	
0xFE0	ROMPIDR0	RO	<i>C8.6 ROM Table Peripheral Identification Register 0 on page C8-383</i>
0xFE4	ROMPIDR1	RO	<i>C8.7 ROM Table Peripheral Identification Register 1 on page C8-384</i>
0xFE8	ROMPIDR2	RO	<i>C8.8 ROM Table Peripheral Identification Register 2 on page C8-385</i>
0xFEC	ROMPIDR3	RO	<i>C8.9 ROM Table Peripheral Identification Register 3 on page C8-386</i>
0xFF0	ROMCIDR0	RO	<i>C8.13 ROM Table Component Identification Register 0 on page C8-390</i>
0xFF4	ROMCIDR1	RO	<i>C8.14 ROM Table Component Identification Register 1 on page C8-391</i>
0xFF8	ROMCIDR2	RO	<i>C8.15 ROM Table Component Identification Register 2 on page C8-392</i>
0xFFC	ROMCIDR3	RO	<i>C8.16 ROM Table Component Identification Register 3 on page C8-393</i>

C8.4 ROM entry registers

The characteristics of the `ROENTRYn` are:

Purpose

Indicates to a debugger whether the debug component is present in the debug logic of the processor. There are 16 `ROENTRY` registers in the Cortex-A34 processor.

Usage constraints

These registers are accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

[C1.4 External access permissions to debug registers on page C1-299](#) describes the condition codes.

Configurations

There is one copy of this register that is used in both Secure and Non-secure states.

Attributes

See [C8.3 ROM table register summary on page C8-378](#).



Figure C8-1 ROMENTRY bit assignments

Address offset, [31:12]

Address offset for the debug component.

Negative values of address offsets are permitted using the two's complement of the offset.

[11:2]

Reserved, `RES0`.

Format, [1]

Format of the ROM table entry. The value for all `ROENTRY` registers is:

- 0 End marker.
- 1 32-bit format.

Component present, [0]

Indicates whether the component is present:

- 0 Component is not present.
- 1 Component is present.

The debug, CTI, and PMU components for core 0 are always present.

The Physical Address of a debug component is determined by shifting the address offset 12 places to the left and adding the result to the Physical Address of the Cortex-A34 processor ROM table.

The following tables show the offset values for all `ROENTRY` values when a v8 memory map is implemented and the offset values for all `ROENTRY` values when a legacy v7 memory map is implemented.

If a core is not implemented, the `ROENTRY` registers for its debug, CTI, PMU, and ETM trace unit components are `0x00000000` when a v8 memory map is implemented and `0x00000002` when a v7 memory map is implemented.

If a core is implemented but the ETM trace unit is not implemented then the corresponding ROMENTRY register is 0x00000002 in both the v7 and v8 memory maps.

Table C8-2 v8 ROMENTRY values

Name	Debug component	Address offset [31:12]	ROMENTRY value
ROMENTRY0	Core 0 Debug	0x00010	0x00010003
ROMENTRY1	Core 0 CTI	0x00020	0x00020003
ROMENTRY2	Core 0 PMU	0x00030	0x00030003
ROMENTRY3	Core 0 ETM	0x00040	0x00040003 If the component is present.
ROMENTRY4	Core 1 Debug	0x00110	0x00110003 If the component is present.
ROMENTRY5	Core 1 CTI	0x00120	0x00120003 If the component is present.
ROMENTRY6	Core 1 PMU	0x00130	0x00130003 If the component is present.
ROMENTRY7	Core 1 ETM	0x00140	0x00140003 If the component is present.
ROMENTRY8	Core 2 Debug	0x00210	0x00210003 If the component is present.
ROMENTRY9	Core 2 CTI	0x00220	0x00220003 If the component is present.
ROMENTRY10	Core 2 PMU	0x00230	0x00230003 If the component is present.
ROMENTRY11	Core 2 ETM	0x00240	0x00240003 If the component is present.
ROMENTRY12	Core 3 Debug	0x00310	0x00310003 If the component is present.
ROMENTRY13	Core 3 CTI	0x00320	0x00320003 If the component is present.
ROMENTRY14	Core 3 PMU	0x00330	0x00330003 If the component is present.
ROMENTRY15	Core 3 ETM	0x00340	0x00340003 If the component is present.

Table C8-3 Legacy v7 ROMENTRY values

Name	Debug component	Address offset [31:12]	ROMENTRY value
ROMENTRY0	Core 0 Debug	0x00010	0x00010003
ROMENTRY1	Core 0 PMU	0x00011	0x00011003
ROMENTRY2	Core 1 Debug	0x00012	0x00012003
ROMENTRY3	Core 1 PMU	0x00013	0x00013003 If the component is present.
ROMENTRY4	Core 2 Debug	0x00014	0x00014003 If the component is present.
ROMENTRY5	Core 2 PMU	0x00015	0x00015003 If the component is present.
ROMENTRY6	Core 3 Debug	0x00016	0x00016003 If the component is present.
ROMENTRY7	Core 3 PMU	0x00017	0x00017003 If the component is present.
ROMENTRY8	Core 0 CTI	0x00018	0x00018003 If the component is present.
ROMENTRY9	Core 1 CTI	0x00019	0x00019003 If the component is present.
ROMENTRY10	Core 2 CTI	0x0001A	0x0001A003 If the component is present.
ROMENTRY11	Core 3 CTI	0x0001B	0x0001B003 If the component is present.
ROMENTRY12	Core 0 ETM	0x0001C	0x0001C003 If the component is present.
ROMENTRY13	Core 1 ETM	0x0001D	0x0001D003 If the component is present.
ROMENTRY14	Core 2 ETM	0x0001E	0x0001E003 If the component is present.
ROMENTRY15	Core 3 ETM	0x0001F	0x0001F003 If the component is present.

C8.5 ROM Table Peripheral Identification Registers

The ROM Table Peripheral Identification Registers provide standard information required for all components that conform to the ARM Debug Interface Architecture Specification, ADIV5.0 to ADIV5.2.

There are eight registers listed in register number order in the following table.

Table C8-4 Summary of the ROM Table Peripheral Identification Registers

Register	Value	Offset
ROMPIDR4	0x04	0xFD0
ROMPIDR5	0x00	0xFD4
ROMPIDR6	0x00	0xFD8
ROMPIDR7	0x00	0xFDC
ROMPIDR0	0xAC for v8 memory map. 0xE2 for v7 memory map.	0xFE0
ROMPIDR1	0xB4	0xFE4
ROMPIDR2	0x1B	0xFE8
ROMPIDR3	0x00	0xFEC

Only bits[7:0] of each Peripheral ID Register are used, with bits[31:8] reserved. Together, the eight Peripheral ID Registers define a single 64-bit Peripheral ID.

C8.6 ROM Table Peripheral Identification Register 0

The ROMPIDR0 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

[C1.4 External access permissions to debug registers on page C1-299](#) describes the condition codes.

Configurations

The ROMPIDR0 is in the Debug power domain.

Attributes

See [C8.3 ROM table register summary on page C8-378](#).

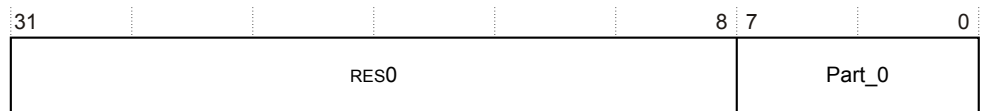


Figure C8-2 ROMPIDR0 bit assignments

[31:8]

Reserved, RES0.

Part_0, [7:0]

Least significant byte of the ROM table part number.

0xAC For v8 memory map.

0xE2 For v7 memory map.

The ROMPIDR0 can be accessed through the external debug interface, offset 0xFE0.

C8.7 ROM Table Peripheral Identification Register 1

The ROMPIDR1 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

[C1.4 External access permissions to debug registers on page C1-299](#) describes the condition codes.

Configurations

The ROMPIDR1 is in the Debug power domain.

Attributes

See [C8.3 ROM table register summary on page C8-378](#).

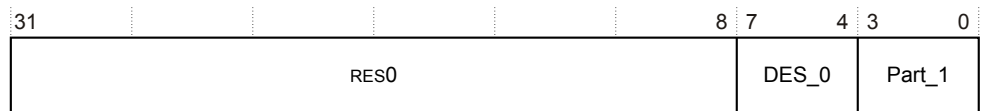


Figure C8-3 ROMPIDR1 bit assignments

[31:8]

Reserved, RES0.

DES_0, [7:4]

0xB Least significant nibble of JEP106 ID code. For ARM Limited.

Part_1, [3:0]

0x4 Most significant nibble of the ROM table part number.

The ROMPIDR1 can be accessed through the external debug interface, offset 0xFE4.

C8.8 ROM Table Peripheral Identification Register 2

The ROMPIDR2 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

C1.4 External access permissions to debug registers on page C1-299 describes the condition codes.

Configurations

The ROMPIDR2 is in the Debug power domain.

Attributes

See *C8.3 ROM table register summary on page C8-378*.

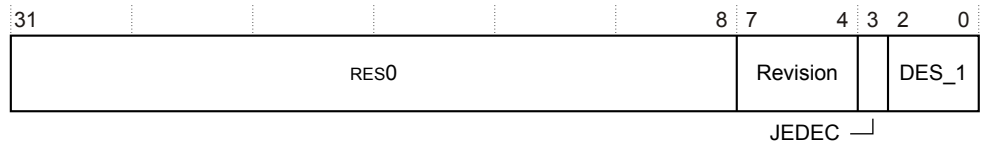


Figure C8-4 ROMPIDR2 bit assignments

[31:8]

Reserved, RES0.

Revision, [7:4]

0x1 r0p1.

JEDEC, [3]

0b1 RAO. Indicates a JEP106 identity code is used.

DES_1, [2:0]

0b011 Designer, most significant bits of JEP106 ID code. For ARM Limited.

The ROMPIDR2 can be accessed through the external debug interface, offset 0xFE8.

C8.9 ROM Table Peripheral Identification Register 3

The ROMPIDR3 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

C1.4 External access permissions to debug registers on page C1-299 describes the condition codes.

Configurations

The ROMPIDR3 is in the Debug power domain.

Attributes

See *C8.3 ROM table register summary on page C8-378*.

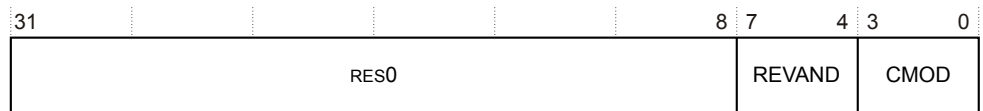


Figure C8-5 ROMPIDR3 bit assignments

[31:8]

Reserved, RES0.

REVAND, [7:4]

0x0 Part minor revision.

CMOD, [3:0]

0x0 Customer modified.

The ROMPIDR3 can be accessed through the external debug interface, offset 0xFEC.

C8.10 ROM Table Peripheral Identification Register 4

The ROMPIDR4 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

C1.4 External access permissions to debug registers on page C1-299 describes the condition codes.

Configurations

The ROMPIDR4 is in the Debug power domain.

Attributes

See *C8.3 ROM table register summary on page C8-378*.

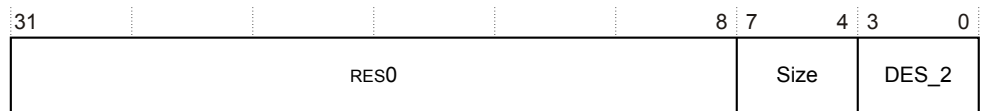


Figure C8-6 ROMPIDR4 bit assignments

[31:8]

Reserved, RES0.

Size, [7:4]

0x0 Size of the component. Log2 the number of 4KB pages from the start of the component to the end of the component ID registers.

DES_2, [3:0]

0x4 Designer, JEP106 continuation code, least significant nibble. For ARM Limited.

The ROMPIDR4 can be accessed through the external debug interface, offset 0xFD0.

C8.11 ROM Table Peripheral Identification Register 5-7

No information is held in the Peripheral ID5, Peripheral ID6, and Peripheral ID7 Registers. They are reserved for future use and are RES0.

C8.12 ROM Table Component Identification Registers

There are four read-only ROM Table Component Identification Registers, Component ID0 through Component ID3.

Table C8-5 Summary of the ROM table component Identification registers

Register	Value	Offset
ROMCIDR0	0x0D	0xFF0
ROMCIDR1	0x10	0xFF4
ROMCIDR2	0x05	0xFF8
ROMCIDR3	0xB1	0xFFC

The ROM Table Component Identification Registers identify Debug as an ARM Debug Interface v5 component.

C8.13 ROM Table Component Identification Register 0

The ROMCIDR0 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

[C1.4 External access permissions to debug registers on page C1-299](#) describes the condition codes.

Configurations

The ROMCIDR0 is in the Debug power domain.

Attributes

See [C8.3 ROM table register summary on page C8-378](#).

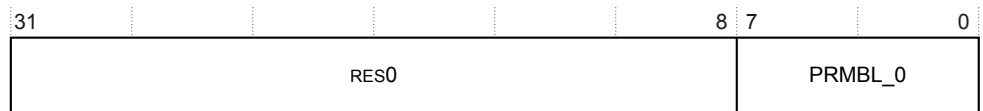


Figure C8-7 ROMCIDR0 bit assignments

[31:8]

Reserved, RES0.

Size, [7:0]

0x0D Preamble byte 0.

The ROMCIDR0 can be accessed through the external debug interface, offset 0xFF0.

C8.14 ROM Table Component Identification Register 1

The ROMCIDR1 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

C1.4 External access permissions to debug registers on page C1-299 describes the condition codes.

Configurations

The ROMCIDR1 is in the Debug power domain.

Attributes

See *C8.3 ROM table register summary on page C8-378*.

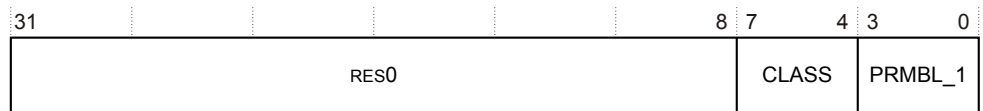


Figure C8-8 ROMCIDR1 bit assignments

[31:8]

Reserved, RES0.

CLASS, [7:4]

0x1 Component Class. For a ROM table.

PRMBL_1, [3:0]

0x0 Preamble.

The ROMCIDR1 can be accessed through the external debug interface, offset 0xFF4.

C8.15 ROM Table Component Identification Register 2

The ROMCIDR2 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

C1.4 External access permissions to debug registers on page C1-299 describes the condition codes.

Configurations

The ROMCIDR2 is in the Debug power domain.

Attributes

See *C8.3 ROM table register summary on page C8-378*.

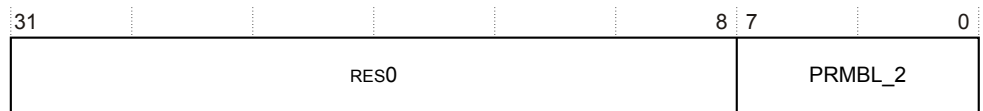


Figure C8-9 ROMCIDR2 bit assignments

[31:8]

Reserved, RES0.

PRMBL_2, [7:0]

0x05 Preamble byte 2.

The ROMCIDR2 can be accessed through the external debug interface, offset 0xFF8.

C8.16 ROM Table Component Identification Register 3

The ROMCIDR3 characteristics are:

Purpose

Provides information to identify an external debug component.

Usage constraints

This register is accessible as follows:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	-	RO

[C1.4 External access permissions to debug registers on page C1-299](#) describes the condition codes.

Configurations

The ROMCIDR3 is in the Debug power domain.

Attributes

See [C8.3 ROM table register summary on page C8-378](#).

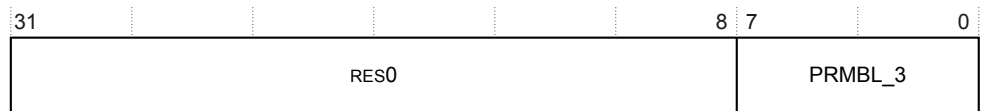


Figure C8-10 ROMCIDR3 bit assignments

[31:8]

Reserved, RES0.

PRMBL_3, [7:0]

0xB1 Preamble byte 3.

The ROMCIDR3 can be accessed through the external debug interface, offset 0xFFC.

Chapter C9

PMU registers

This chapter describes the PMU registers.

It contains the following sections:

- *C9.1 AArch64 PMU register summary* on page C9-396.
- *C9.2 Performance Monitors Control Register, EL0* on page C9-397.
- *C9.3 Performance Monitors Common Event Identification Register 0, EL0* on page C9-399.
- *C9.4 Performance Monitors Common Event Identification Register 1, EL0* on page C9-403.
- *C9.5 Memory-mapped PMU register summary* on page C9-405.
- *C9.6 Performance Monitors Configuration Register* on page C9-408.
- *C9.7 Performance Monitors Peripheral Identification Registers* on page C9-409.
- *C9.8 Performance Monitors Peripheral Identification Register 0* on page C9-410.
- *C9.9 Performance Monitors Peripheral Identification Register 1* on page C9-411.
- *C9.10 Performance Monitors Peripheral Identification Register 2* on page C9-412.
- *C9.11 Performance Monitors Peripheral Identification Register 3* on page C9-413.
- *C9.12 Performance Monitors Peripheral Identification Register 4* on page C9-414.
- *C9.13 Performance Monitors Peripheral Identification Register 5-7* on page C9-415.
- *C9.14 Performance Monitors Component Identification Registers* on page C9-416.
- *C9.15 Performance Monitors Component Identification Register 0* on page C9-417.
- *C9.16 Performance Monitors Component Identification Register 1* on page C9-418.
- *C9.17 Performance Monitors Component Identification Register 2* on page C9-419.
- *C9.18 Performance Monitors Component Identification Register 3* on page C9-420.

C9.1 AArch64 PMU register summary

The PMU counters and their associated control registers are accessible in the AArch64 Execution state with MRS and MSR instructions.

The following table gives a summary of the Cortex-A34 PMU registers in the AArch64 Execution state. For those registers not described in this chapter, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

Table C9-1 PMU register summary in the AArch64 Execution state

Name	Type	Width	Description
PMCR_EL0	RW	32	C9.2 Performance Monitors Control Register, EL0 on page C9-397
PMCNTENSET_EL0	RW	32	Performance Monitors Count Enable Set Register
PMCNTENCLR_EL0	RW	32	Performance Monitors Count Enable Clear Register
PMOVSCLR_EL0	RW	32	Performance Monitors Overflow Flag Status Register
PMSWINC_EL0	WO	32	Performance Monitors Software Increment Register
PMSELR_EL0	RW	32	Performance Monitors Event Counter Selection Register
PMCEID0_EL0	RO	32	C9.3 Performance Monitors Common Event Identification Register 0, EL0 on page C9-399
PMCEID1_EL0	RO	32	C9.4 Performance Monitors Common Event Identification Register 1, EL0 on page C9-403
PMCCNTR_EL0	RW	64	Performance Monitors Cycle Count Register
PMXEVTYPER_EL0	RW	32	Performance Monitors Selected Event Type and Filter Register
PMCCFILTR_EL0	RW	32	Performance Monitors Cycle Count Filter Register
PMXEVCNTR0_EL0	RW	32	Performance Monitors Selected Event Count Register
PMUSERENR_EL0	RW	32	Performance Monitors User Enable Register
PMINTENSET_EL1	RW	32	Performance Monitors Interrupt Enable Set Register
PMINTENCLR_EL1	RW	32	Performance Monitors Interrupt Enable Clear Register
PMOVSSET_EL0	RW	32	Performance Monitors Overflow Flag Status Set Register
PMEVCNTR0_EL0	RW	32	Performance Monitors Event Count Registers
PMEVCNTR1_EL0	RW	32	
PMEVCNTR2_EL0	RW	32	
PMEVCNTR3_EL0	RW	32	
PMEVCNTR4_EL0	RW	32	
PMEVCNTR5_EL0	RW	32	
PMEVTYPER0_EL0	RW	32	Performance Monitors Event Type Registers
PMEVTYPER1_EL0	RW	32	
PMXVTYPER2_EL0	RW	32	
PMEVTYPER3_EL0	RW	32	
PMEVTYPER4_EL0	RW	32	
PMEVTYPER5_EL0	RW	32	
PMCCFILTR_EL0	RW	32	Performance Monitors Cycle Count Filter Register

C9.2 Performance Monitors Control Register, EL0

The PMCR_EL0 characteristics are:

Purpose

Provides details of the Performance Monitors implementation, including the number of counters implemented, and configures and controls the counters.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
RW	RW	RW	RW	RW	RW

This register is accessible at EL0 when PMUSERENR_EL0.EN is set to 1.

Configurations

PMCR[6:0] is architecturally mapped to external PMCR_EL0 register.

Attributes

PMCR_EL0 is a 32-bit register.

31	24	23	16	15	11	10	7	6	5	4	3	2	1	0				
IMP				IDCODE				N		RES0		LC	DP	X	D	C	P	E

Figure C9-1 PMCR_EL0 bit assignments

IMP, [31:24]

Implementer code:

0x41 ARM.

This is a read-only field.

IDCODE, [23:16]

Identification code:

0x08 Cortex-A34.

This is a read-only field.

N, [15:11]

Number of event counters.

0b00110 Six counters.

[10:7]

Reserved, RES0.

LC, [6]

Reserved, RES1.

DP, [5]

Disable cycle counter, PMCCNTR_EL0 when event counting is prohibited:

0 Cycle counter operates regardless of the non-invasive debug authentication settings. This is the reset value.

1 Cycle counter is disabled if non-invasive debug is not permitted and enabled.

This bit is read/write.

X, [4]

Export enable. This bit permits events to be exported to another debug device, such as a trace macrocell, over an event bus:

- 0 Export of events is disabled. This is the reset value.
- 1 Export of events is enabled.

This bit is read/write and does not affect the generation of Performance Monitors interrupts on the **nPMUIRQ** pin.

D, [3]

Reserved, RES0.

C, [2]

Clock counter reset. This bit is WO. The effects of writing to this bit are:

- 0 No action. This is the reset value.
- 1 Reset PMCCNTR_EL0 to 0.

This bit is always RAZ.

Resetting PMCCNTR_EL0 does not clear the PMCCNTR_EL0 overflow bit to 0. See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

P, [1]

Event counter reset. This bit is WO. The effects of writing to this bit are:

- 0 No action. This is the reset value.
- 1 Reset all event counters, not including PMCCNTR_EL0, to zero.

This bit is always RAZ.

In Non-secure EL0 and EL1, a write of 1 to this bit does not reset event counters that MDCR_EL2.HPMN reserves for EL2 use.

In EL2 and EL3, a write of 1 to this bit resets all the event counters.

Resetting the event counters does not clear any overflow bits to 0.

E, [0]

Enable. The possible values of this bit are:

- 0 All counters, including PMCCNTR_EL0, are disabled. This is the reset value.
- 1 All counters are enabled.

This bit is RW.

In Non-secure EL0 and EL1, this bit does not affect the operation of event counters that MDCR_EL2.HPMN reserves for EL2 use.

On Warm reset, the field resets to 0.

To access the PMCR_EL0:

```
MRS <Xt>, PMCR_EL0 ; Read PMCR_EL0 into Xt
MSR PMCR_EL0, <Xt> ; Write Xt to PMCR_EL0
```

```
MRC p15, 0, <Rt>, c9, c12, 0; Read Performance Monitor Control Register
MCR p15, 0, <Rt>, c9, c12, 0; Write Performance Monitor Control Register
```

The PMCR_EL0 can be accessed through the external debug interface, offset 0xE04.

C9.3 Performance Monitors Common Event Identification Register 0, EL0

The PMCEID0_EL0 characteristics are:

Purpose

Defines which common architectural and common microarchitectural feature events are implemented.

Usage constraints

This register is accessible as follows:

EL0	EL1	EL1	EL2	EL3	EL3
	(NS)	(S)		(SCR.NS = 1)	(SCR.NS = 0)
Config	RO	RO	RO	RO	RO

This register is accessible at EL0 when PMUSERENR_EL0.EN is set to 1.

Configurations

The PMCEID0_EL0 is architecturally mapped to the external register PMCEID0_EL0.

Attributes

PMCEID0_EL0 is a 32-bit register.

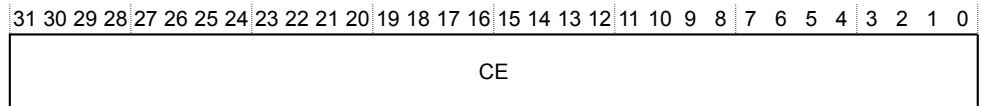


Figure C9-2 PMCEID0_EL0 bit assignments

CE[31:0], [31:0]

Common architectural and microarchitectural feature events that can be counted by the PMU event counters.

For each bit described in the following table, the event is implemented if the bit is set to 1, or not implemented if the bit is set to 0.

Table C9-2 PMU common events

Bit	Event number	Event mnemonic	Description
[31]	0x1F	L1D_CACHE_ALLOCATE	L1 Data cache allocate: 0 This event is not implemented.
[30]	0x1E	CHAIN	Chain. For odd-numbered counters, counts once for each overflow of the preceding even-numbered counter. For even-numbered counters, does not count: 1 This event is implemented.
[29]	0x1D	BUS_CYCLES	Bus cycle: 1 This event is implemented.
[28]	0x1C	TTBR_WRITE_RETIRED	TTBR write, architecturally executed, condition check pass - write to translation table base: 0 This event is not implemented.
[27]	0x1B	INST_SPEC	Instruction speculatively executed: 1 This event is implemented.

Table C9-2 PMU common events (continued)

Bit	Event number	Event mnemonic	Description
[26]	0x1A	MEMORY_ERROR	Local memory error: 1 This event is implemented.
[25]	0x19	BUS_ACCESS	Bus access: 1 This event is implemented.
[24]	0x18	L2D_CACHE_WB	L2 Data cache Write-Back: 0 This event is not implemented if the Cortex-A34 processor has been configured without an L2 cache. 1 This event is implemented if the Cortex-A34 processor has been configured with an L2 cache.
[23]	0x17	L2D_CACHE_REFILL	L2 Data cache refill: 0 This event is not implemented if the Cortex-A34 processor has been configured without an L2 cache. 1 This event is implemented if the Cortex-A34 processor has been configured with an L2 cache.
[22]	0x16	L2D_CACHE	L2 Data cache access: 0 This event is not implemented if the Cortex-A34 processor has been configured without an L2 cache. 1 This event is implemented if the Cortex-A34 processor has been configured with an L2 cache.
[21]	0x15	L1D_CACHE_WB	L1 Data cache Write-Back: 1 This event is implemented.
[20]	0x14	L1I_CACHE	L1 Instruction cache access: 1 This event is implemented.
[19]	0x13	MEM_ACCESS	Data memory access: 1 This event is implemented.
[18]	0x12	BR_PRED	Predictable branch speculatively executed: 1 This event is implemented.
[17]	0x11	CPU_CYCLES	Cycle: 1 This event is implemented.
[16]	0x10	BR_MIS_PRED	Mispredicted or not predicted branch speculatively executed: 1 This event is implemented.
[15]	0x0F	UNALIGNED_LDST_RETIRED	Instruction architecturally executed, condition check pass - unaligned load or store: 1 This event is implemented.

Table C9-2 PMU common events (continued)

Bit	Event number	Event mnemonic	Description
[14]	0x0E	BR_RETURN_RETIRED	Instruction architecturally executed, condition check pass - procedure return: 0 This event is not implemented.
[13]	0x0D	BR_IMMED_RETIRED	Instruction architecturally executed - immediate branch: 1 This event is implemented.
[12]	0x0C	PC_WRITE_RETIRED	Instruction architecturally executed, condition check pass - software change of the PC: 1 This event is implemented.
[11]	0x0B	CID_WRITE_RETIRED	Instruction architecturally executed, condition check pass - write to CONTEXTIDR: 1 This event is implemented.
[10]	0x0A	EXC_RETURN	Instruction architecturally executed, condition check pass - exception return: 1 This event is implemented.
[9]	0x09	EXC_TAKEN	Exception taken: 1 This event is implemented.
[8]	0x08	INST_RETIRED	Instruction architecturally executed: 1 This event is implemented.
[7]	0x07	ST_RETIRED	Instruction architecturally executed, condition check pass - store: 1 This event is implemented.
[6]	0x06	LD_RETIRED	Instruction architecturally executed, condition check pass - load: 1 This event is implemented.
[5]	0x05	L1D_TLB_REFILL	L1 Data TLB refill: 1 This event is implemented.
[4]	0x04	L1D_CACHE	L1 Data cache access: 1 This event is implemented.
[3]	0x03	L1D_CACHE_REFILL	L1 Data cache refill: 1 This event is implemented.
[2]	0x02	L1I_TLB_REFILL	L1 Instruction TLB refill: 1 This event is implemented.

Table C9-2 PMU common events (continued)

Bit	Event number	Event mnemonic	Description
[1]	0x01	L1I_CACHE_REFILL	L1 Instruction cache refill: 1 This event is implemented.
[0]	0x00	SW_INCR	Instruction architecturally executed, condition check pass - software increment: 1 This event is implemented.

To access the PMCEID0_EL0:

MRS <Xt>, PMCEID0_EL0; Read Performance Monitor Common Event Identification Register 0

The PMCEID0_EL0 can be accessed through the external debug interface, offset 0xE20.

C9.4 Performance Monitors Common Event Identification Register 1, EL0

The PMCEID1_EL0 characteristics are:

Purpose

Defines which common architectural and common microarchitectural feature events are implemented.

Usage constraints

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
Config	RO	RO	RO	RO	RO

This register is accessible at EL0 when PMUSERENR_EL0.EN is set to 1.

Configurations

The PMCEID1_EL0 is architecturally mapped to the external register PMCEID1_EL0.

Attributes

PMCEID1_EL0 is a 32-bit register.

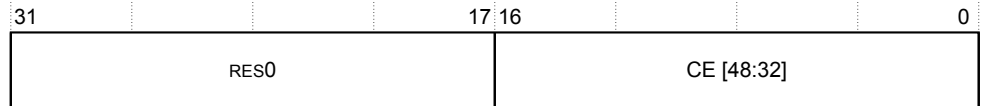


Figure C9-3 PMCEID1 bit assignments

[31:17]

RES0.

CE[48:32], [16:0]

Common architectural and microarchitectural feature events that can be counted by the PMU event counters.

For each bit described in The following table, the event is implemented if the bit is set to 1, or not implemented if the bit is set to 0.

Table C9-3 PMU common events

Bit	Event number	Event mnemonic	Description
[16]	0x30	L2I_TLB	Attributable Level 2 instruction TLB access. 0 This event is not implemented.
[15]	0x2F	L2D_TLB	Attributable Level 2 data or unified TLB access. 0 This event is not implemented.
[14]	0x2E	L2I_TLB_REFILL	Attributable Level 2 instruction TLB refill. 0 This event is not implemented.
[13]	0x2D	L2D_TLB_REFIL	Attributable Level 2 data or unified TLB refill. 0 This event is not implemented.
[12]	0x2C	L3D_CACHE_WB	Attributable Level 3 data or unified cache write-back. 0 This event is not implemented.

Table C9-3 PMU common events (continued)

Bit	Event number	Event mnemonic	Description
[11]	0x2B	L3D_CACHE	Attributable Level 3 data or unified cache access. 0 This event is not implemented.
[10]	0x2A	L3D_CACHE_REFILL	Attributable Level 3 data or unified cache refill. 0 This event is not implemented.
[9]	0x29	L3D_CACHE_ALLOCATE	Attributable Level 3 data or unified cache allocation without refill. 0 This event is not implemented.
[8]	0x28	L2I_CACHE_REFILL	Attributable Level 2 instruction cache refill. 0 This event is not implemented.
[7]	0x27	L2I_CACHE	Attributable Level 2 instruction cache access. 0 This event is not implemented.
[6]	0x26	L1I_TLB	Level 1 instruction TLB access. 0 This event is not implemented.
[5]	0x25	L1D_TLB	Level 1 data or unified TLB access. 0 This event is not implemented.
[4]	0x24	STALL_BACKEND	No operation issued due to backend. 0 This event is not implemented.
[3]	0x23	STALL_FRONTEND	No operation issued due to the frontend. 0 This event is not implemented.
[2]	0x22	BR_MIS_PRED_RETIRE	Instruction architecturally executed, mispredicted branch. 0 This event is not implemented.
[1]	0x21	BR_RETIRE	Instruction architecturally executed, branch. 0 This event is not implemented.
[0]	0x20	L2D_CACHE_ALLOCATE	Level 2 data cache allocation without refill. 0 This event is not implemented.

To access the PMCEID1_EL0:

```
MRS <Xt>, PMCEID1_EL0; Read Performance Monitor Common Event Identification Register 0
```

The PMCEID1_EL0 can be accessed through the external debug interface, offset 0xE24.

C9.5 Memory-mapped PMU register summary

There are PMU registers that are accessible through the external debug interface.

These registers are listed in the following table. For those registers not described in this chapter, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

Table C9-4 Memory-mapped PMU register summary

Offset	Name	Type	Description
0x000	PMEVCNTR0_EL0	RW	Performance Monitors Event Count Register 0
0x004	-	-	Reserved
0x008	PMEVCNTR1_EL0	RW	Performance Monitors Event Count Register 1
0x00C	-	-	Reserved
0x010	PMEVCNTR2_EL0	RW	Performance Monitors Event Count Register 2
0x014	-	-	Reserved
0x018	PMEVCNTR3_EL0	RW	Performance Monitors Event Count Register 3
0x01C	-	-	Reserved
0x020	PMEVCNTR4_EL0	RW	Performance Monitors Event Count Register 4
0x024	-	-	Reserved
0x028	PMEVCNTR5_EL0	RW	Performance Monitors Event Count Register 5
0x02C-0xF4	-	-	Reserved
0x0F8	PMCCNTR_EL0[31:0]	RW	Performance Monitors Cycle Count Register
0x0FC	PMCCNTR_EL0[63:32]	RW	
0x100-0x3FC	-	-	Reserved
0x400	PMEVTYPER0_EL0	RW	Performance Monitors Event Type Register
0x404	PMEVTYPER1_EL0	RW	
0x408	PMEVTYPER2_EL0	RW	
0x40C	PMEVTYPER3_EL0	RW	
0x410	PMEVTYPER4_EL0	RW	
0x414	PMEVTYPER5_EL0	RW	
0x418-0x478	-	-	Reserved
0x47C	PMCCFILTR_EL0	RW	Performance Monitors Cycle Count Filter Register
0x480-0xBFC	-	-	Reserved
0xC00	PMCNTENSET_EL0	RW	Performance Monitors Count Enable Set Register
0xC04-0xC1C	-	-	Reserved
0xC20	PMCNTENCLR_EL0	RW	Performance Monitors Count Enable Clear Register
0xC24-0xC3C	-	-	Reserved
0xC40	PMINTENSET_EL1	RW	Performance Monitors Interrupt Enable Set Register
0xC44-0xC5C	-	-	Reserved

Table C9-4 Memory-mapped PMU register summary (continued)

Offset	Name	Type	Description
0xC60	PMINTENCLR_EL1	RW	Performance Monitors Interrupt Enable Clear Register
0xC64-0xC7C	-	-	Reserved
0xC80	PMOVSLR_EL0	RW	Performance Monitors Overflow Flag Status Register
0xC84-0xC9C	-	-	Reserved
0xCA0	PMSWINC_EL0	WO	Performance Monitors Software Increment Register
0xCA4-0xCBC	-	-	Reserved
0xCC0	PMOVSSET_EL0	RW	Performance Monitors Overflow Flag Status Set Register
0xCC4-0xDFC	-	-	Reserved
0xE00	PMCFGR	RO	<i>C9.6 Performance Monitors Configuration Register on page C9-408</i>
0xE04	PMCR_EL0	RW	Performance Monitors Control Register
0xE08-0xE1C	-	-	Reserved
0xE20	PMCEID0_EL0	RO	<i>C9.3 Performance Monitors Common Event Identification Register 0, EL0 on page C9-399</i>
0xE24	PMCEID1_EL0	RO	<i>C9.4 Performance Monitors Common Event Identification Register 1, EL0 on page C9-403</i>
0xE28-0xFA4	-	-	Reserved
0xFA8	PMDEVAFF0	RO	Performance Monitors Device Affinity Register 0, see <i>B1.65 Multiprocessor Affinity Register, EL1 on page B1-245</i>
0xFAC	PMDEVAFF1	RO	Performance Monitors Device Affinity Register 1, see <i>B1.65 Multiprocessor Affinity Register, EL1 on page B1-245</i>
0xFB0	PMLAR	WO	Performance Monitors Lock Access Register
0xFB4	PMLSR	RO	Performance Monitors Lock Status Register
0xFB8	PMAUTHSTATUS	RO	Performance Monitors Authentication Status Register
0xFBC	PMDEVARCH		Performance Monitors Device Architecture Register
0xFC0-0xFC8	-	-	Reserved
0xFCC	PMDEVTYPE	RO	Performance Monitors Device Type Register
0xFD0	PMPIDR4	RO	<i>C9.12 Performance Monitors Peripheral Identification Register 4 on page C9-414</i>
0xFD4	PMPIDR5	RO	<i>C9.13 Performance Monitors Peripheral Identification Register 5-7 on page C9-415</i>
0xFD8	PMPIDR6	RO	
0xFDC	PMPIDR7	RO	
0xFE0	PMPIDR0	RO	<i>C9.8 Performance Monitors Peripheral Identification Register 0 on page C9-410</i>
0xFE4	PMPIDR1	RO	<i>C9.9 Performance Monitors Peripheral Identification Register 1 on page C9-411</i>
0xFE8	PMPIDR2	RO	<i>C9.10 Performance Monitors Peripheral Identification Register 2 on page C9-412</i>
0xFEC	PMPIDR3	RO	<i>C9.11 Performance Monitors Peripheral Identification Register 3 on page C9-413</i>
0xFF0	PMCIDR0	RO	<i>C9.15 Performance Monitors Component Identification Register 0 on page C9-417</i>
0xFF4	PMCIDR1	RO	<i>C9.16 Performance Monitors Component Identification Register 1 on page C9-418</i>

Table C9-4 Memory-mapped PMU register summary (continued)

Offset	Name	Type	Description
0xFF8	PMCIDR2	RO	<i>C9.17 Performance Monitors Component Identification Register 2 on page C9-419</i>
0xFFC	PMCIDR3	RO	<i>C9.18 Performance Monitors Component Identification Register 3 on page C9-420</i>

C9.6 Performance Monitors Configuration Register

The PMCFGR characteristics are:

Purpose

Contains PMU specific configuration data.

Usage constraints

The accessibility to the PMCFGR by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
Error	Error	Error	Error	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMCFGR is in the processor power domain.

Attributes

See [C9.5 Memory-mapped PMU register summary on page C9-405](#).

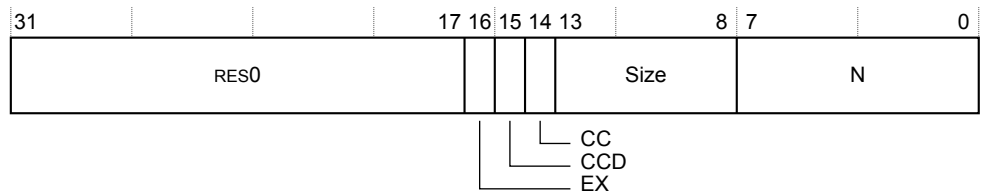


Figure C9-4 PMCFGR bit assignments

[31:17]

Reserved, RES0.

EX, [16]

Export supported. The value is:

1 Export is supported. PMCR_EL0.EX is read/write.

CCD, [15]

Cycle counter has pre-scale. The value is:

1 PMCR_EL0.D is read/write.

CC, [14]

Dedicated cycle counter supported. The value is:

1 Dedicated cycle counter is supported.

Size, [13:8]

Counter size. The value is:

0b111111 64-bit counters.

N, [7:0]

Number of event counters. The value is:

0x06 Six counters.

The PMCFGR can be accessed through the external debug interface, offset 0xE00.

C9.7 Performance Monitors Peripheral Identification Registers

The Performance Monitors Peripheral Identification Registers provide standard information required for all components that conform to the ARM PMUv3 architecture.

The following table lists the Performance Monitors Peripheral Identification Registers.

Table C9-5 Summary of the Performance Monitors Peripheral Identification Registers

Register	Value	Offset
Peripheral ID4	0x04	0xFD0
Peripheral ID5	0x00	0xFD4
Peripheral ID6	0x00	0xFD8
Peripheral ID7	0x00	0xFDC
Peripheral ID0	0xDC	0xFE0
Peripheral ID1	0xB9	0xFE4
Peripheral ID2	0x1B	0xFE8
Peripheral ID3	0x00	0xFEC

Only bits[7:0] of each Peripheral ID Register are used, with bits[31:8] reserved. Together, the eight Peripheral ID Registers define a single 64-bit Peripheral ID.

C9.8 Performance Monitors Peripheral Identification Register 0

The PMPIDR0 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMPIDR0 can be accessed through the external debug interface.

The accessibility to the PMPIDR0 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMPIDR0 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

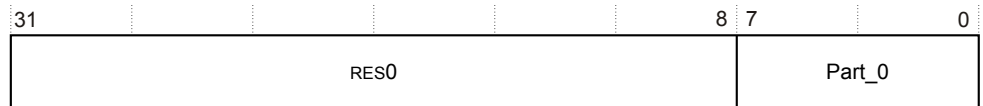


Figure C9-5 PMPIDR0 bit assignments

[31:8]

Reserved, RES0.

Part_0, [7:0]

0xDC Least significant byte of the performance monitor part number.

The PMPIDR0 can be accessed through the external debug interface, offset 0xFE0.

C9.9 Performance Monitors Peripheral Identification Register 1

The PMPIDR1 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMPIDR1 can be accessed through the external debug interface.

The accessibility to the PMPIDR1 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMPIDR1 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

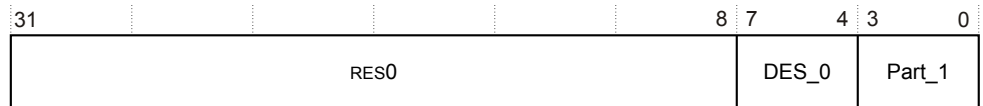


Figure C9-6 PMPIDR1 bit assignments

[31:8]

Reserved, RES0.

DES_0, [7:4]

0xB ARM Limited. This is the least significant nibble of JEP106 ID code.

Part_1, [3:0]

0x9 Most significant nibble of the performance monitor part number.

The PMPIDR1 can be accessed through the external debug interface, offset 0xFE4.

C9.10 Performance Monitors Peripheral Identification Register 2

The PMPIDR2 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The accessibility to the PMPIDR2 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

The PMPIDR2 can be accessed through the external debug interface.

Configurations

The PMPIDR2 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

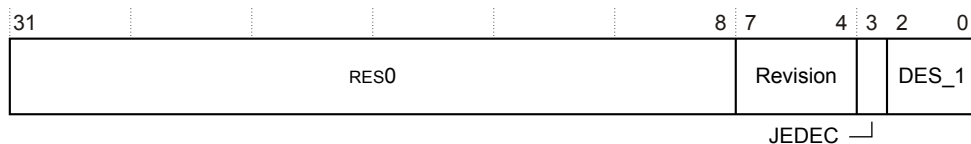


Figure C9-7 PMPIDR2 bit assignments

[31:8]

Reserved, RES0.

Revision, [7:4]

0x1 r0p1.

JEDEC, [3]

0b1 RAO. Indicates a JEP106 identity code is used.

DES_1, [2:0]

0b011 ARM Limited. This is the most significant nibble of JEP106 ID code.

The PMPIDR2 can be accessed through the external debug interface, offset 0xFE8.

C9.11 Performance Monitors Peripheral Identification Register 3

The PMPIDR3 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMPIDR3 can be accessed through the external debug interface.

The accessibility to the PMPIDR3 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMPIDR3 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

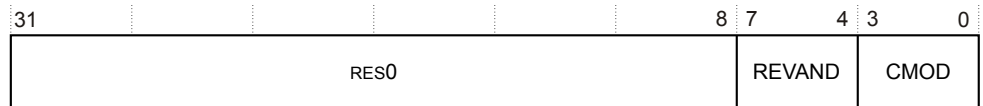


Figure C9-8 PMPIDR3 bit assignments

[31:8]

Reserved, RES0.

REVAND, [7:4]

0x0 Part minor revision.

CMOD, [3:0]

0x0 Customer modified.

The PMPIDR3 can be accessed through the external debug interface, offset 0xFEC.

C9.12 Performance Monitors Peripheral Identification Register 4

The PMPIDR4 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMPIDR4 can be accessed through the external debug interface.

The accessibility to the PMPIDR4 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMPIDR4 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

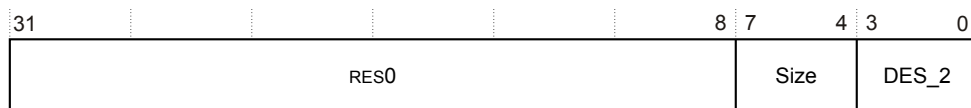


Figure C9-9 PMPIDR4 bit assignments

[31:8]

Reserved, RES0.

Size, [7:4]

0x0 Size of the component. Log2 the number of 4KB pages from the start of the component to the end of the component ID registers.

DES_2, [3:0]

0x4 ARM Limited. This is the least significant nibble JEP106 continuation code.

The PMPIDR4 can be accessed through the external debug interface, offset 0xFD0.

C9.13 Performance Monitors Peripheral Identification Register 5-7

No information is held in the Peripheral ID5, Peripheral ID6, and Peripheral ID7 Registers. They are reserved for future use and are RES0.

C9.14 Performance Monitors Component Identification Registers

There are four read-only PMU Component Identification Registers, Component ID0 through Component ID3.

Table C9-6 Summary of the Performance Monitors Component Identification Registers

Register	Value	Offset
Component ID0	0x0D	0xFF0
Component ID1	0x90	0xFF4
Component ID2	0x05	0xFF8
Component ID3	0xB1	0xFFC

The Performance Monitors Component Identification Registers identify Performance Monitor as ARM PMUv3 architecture.

C9.15 Performance Monitors Component Identification Register 0

The PMCIDR0 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMCIDR0 can be accessed through the external debug interface.

The accessibility to the PMCIDR0 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMCIDR0 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

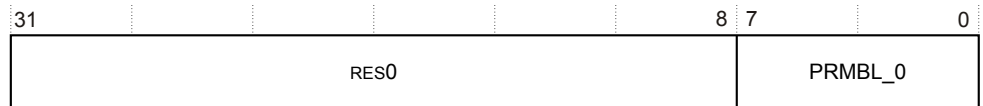


Figure C9-10 PMCIDR0 bit assignments

[31:8]

Reserved, RES0.

Size, [7:0]

0x0D Preamble byte 0.

The PMCIDR0 can be accessed through the external debug interface, offset 0xFF0.

C9.16 Performance Monitors Component Identification Register 1

The PMCIDR1 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMCIDR1 can be accessed through the external debug interface.

The accessibility to the PMCIDR1 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMCIDR1 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

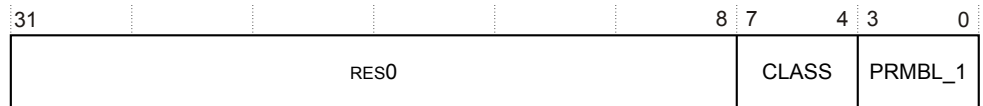


Figure C9-11 PMCIDR1 bit assignments

[31:8]

Reserved, RES0.

CLASS, [7:4]

0x9 Debug component.

PRMBL_1, [3:0]

0x0 Preamble byte 1.

The PMCIDR1 can be accessed through the external debug interface, offset 0xFF4.

C9.17 Performance Monitors Component Identification Register 2

The PMCIDR2 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMCIDR2 can be accessed through the external debug interface.

The accessibility to the PMCIDR2 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMCIDR2 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

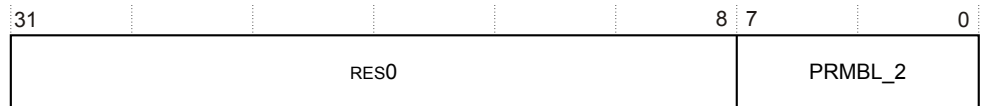


Figure C9-12 PMCIDR2 bit assignments

[31:8]

Reserved, RES0.

PRMBL_2, [7:0]

0x05 Preamble byte 2.

The PMCIDR2 can be accessed through the external debug interface, offset 0xFF8.

C9.18 Performance Monitors Component Identification Register 3

The PMCIDR3 characteristics are:

Purpose

Provides information to identify a Performance Monitor component.

Usage constraints

The PMCIDR3 can be accessed through the external debug interface.

The accessibility to the PMCIDR3 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

[C2.2 External register access permissions to the PMU registers on page C2-307](#) describes the condition codes.

Configurations

The PMCIDR3 is in the Debug power domain.

Attributes

See the register summary in [C9.5 Memory-mapped PMU register summary on page C9-405](#).

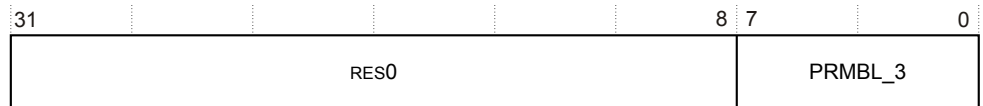


Figure C9-13 PMCIDR3 bit assignments

[31:8]

Reserved, RES0.

PRMBL_3, [7:0]

0xB1 Preamble byte 3.

The PMCIDR3 can be accessed through the external debug interface, offset 0xFFC.

Chapter C10

ETM registers

This chapter describes the ETM registers.

It contains the following sections:

- *C10.1 ETM register summary* on page C10-423.
- *C10.2 Programming Control Register* on page C10-426.
- *C10.3 Status Register* on page C10-427.
- *C10.4 Trace Configuration Register* on page C10-428.
- *C10.5 Branch Broadcast Control Register* on page C10-430.
- *C10.6 Auxiliary Control Register* on page C10-431.
- *C10.7 Event Control 0 Register* on page C10-433.
- *C10.8 Event Control 1 Register* on page C10-435.
- *C10.9 Stall Control Register* on page C10-436.
- *C10.10 Global Timestamp Control Register* on page C10-437.
- *C10.11 Synchronization Period Register* on page C10-438.
- *C10.12 Cycle Count Control Register* on page C10-439.
- *C10.13 Trace ID Register* on page C10-440.
- *C10.14 ViewInst Main Control Register* on page C10-441.
- *C10.15 ViewInst Include-Exclude Control Register* on page C10-443.
- *C10.16 ViewInst Start-Stop Control Register* on page C10-444.
- *C10.17 Sequencer State Transition Control Registers 0-2* on page C10-445.
- *C10.18 Sequencer Reset Control Register* on page C10-447.
- *C10.19 Sequencer State Register* on page C10-448.
- *C10.20 External Input Select Register* on page C10-449.
- *C10.21 Counter Reload Value Registers 0-1* on page C10-450.
- *C10.22 Counter Control Register 0* on page C10-451.
- *C10.23 Counter Control Register 1* on page C10-452.

- *C10.24 Counter Value Registers 0-1* on page C10-454.
- *C10.25 ID Register 8* on page C10-455.
- *C10.26 ID Register 9* on page C10-456.
- *C10.27 ID Register 10* on page C10-457.
- *C10.28 ID Register 11* on page C10-458.
- *C10.29 ID Register 12* on page C10-459.
- *C10.30 ID Register 13* on page C10-460.
- *C10.31 Implementation Specific Register 0* on page C10-461.
- *C10.32 ID Register 0* on page C10-462.
- *C10.33 ID Register 1* on page C10-464.
- *C10.34 ID Register 2* on page C10-465.
- *C10.35 ID Register 3* on page C10-466.
- *C10.36 ID Register 4* on page C10-468.
- *C10.37 ID Register 5* on page C10-469.
- *C10.38 Resource Selection Control Registers 2-16* on page C10-471.
- *C10.39 Single-Shot Comparator Control Register 0* on page C10-472.
- *C10.40 Single-Shot Comparator Status Register 0* on page C10-473.
- *C10.41 OS Lock Access Register* on page C10-474.
- *C10.42 OS Lock Status Register* on page C10-475.
- *C10.43 Power Down Control Register* on page C10-476.
- *C10.44 Power Down Status Register* on page C10-477.
- *C10.45 Address Comparator Value Registers 0-7* on page C10-478.
- *C10.46 Address Comparator Access Type Registers 0-7* on page C10-479.
- *C10.47 Context ID Comparator Value Register 0* on page C10-481.
- *C10.48 VMID Comparator Value Register 0* on page C10-482.
- *C10.49 Context ID Comparator Control Register 0* on page C10-483.
- *C10.50 Integration ATB Identification Register* on page C10-484.
- *C10.51 Integration Instruction ATB Data Register* on page C10-485.
- *C10.52 Integration Instruction ATB In Register* on page C10-486.
- *C10.53 Integration Instruction ATB Out Register* on page C10-487.
- *C10.54 Integration Mode Control Register* on page C10-488.
- *C10.55 Claim Tag Set Register* on page C10-489.
- *C10.56 Claim Tag Clear Register* on page C10-490.
- *C10.57 Device Affinity Register 0* on page C10-491.
- *C10.58 Device Affinity Register 1* on page C10-493.
- *C10.59 Software Lock Access Register* on page C10-494.
- *C10.60 Software Lock Status Register* on page C10-495.
- *C10.61 Authentication Status Register* on page C10-496.
- *C10.62 Device Architecture Register* on page C10-497.
- *C10.63 Device ID Register* on page C10-498.
- *C10.64 Device Type Register* on page C10-499.
- *C10.65 ETM Peripheral Identification Registers* on page C10-500.
- *C10.66 ETM Peripheral Identification Register 0* on page C10-501.
- *C10.67 ETM Peripheral Identification Register 1* on page C10-502.
- *C10.68 ETM Peripheral Identification Register 2* on page C10-503.
- *C10.69 ETM Peripheral Identification Register 3* on page C10-504.
- *C10.70 ETM Peripheral Identification Register 4* on page C10-505.
- *C10.71 ETM Peripheral Identification Register 5-7* on page C10-506.
- *C10.72 ETM Component Identification Registers* on page C10-507.
- *C10.73 ETM Component Identification Register 0* on page C10-508.
- *C10.74 ETM Component Identification Register 1* on page C10-509.
- *C10.75 ETM Component Identification Register 2* on page C10-510.
- *C10.76 ETM Component Identification Register 3* on page C10-511.

C10.1 ETM register summary

This section summarizes the ETM trace unit registers.

All ETM trace unit registers are 32 bits wide. The description of each register includes its offset from a base address. The base address is defined by the system integrator when placing the ETM trace unit in the Debug-APB memory map.

Table C10-1 ETM trace unit register summary

Name	Type	Description
TRCPRGCTLR	RW	<i>C10.2 Programming Control Register on page C10-426</i>
TRCSTATR	RO	<i>C10.3 Status Register on page C10-427</i>
TRCCONFIGR	RW	<i>C10.4 Trace Configuration Register on page C10-428</i>
TRCAUXCTLR	RW	<i>C10.6 Auxiliary Control Register on page C10-431</i>
TRCEVENTCTL0R	RW	<i>C10.7 Event Control 0 Register on page C10-433</i>
TRCEVENTCTL1R	RW	<i>C10.8 Event Control 1 Register on page C10-435</i>
TRCSTALLCTLR	RW	<i>C10.9 Stall Control Register on page C10-436</i>
TRCTSCTLR	RW	<i>C10.10 Global Timestamp Control Register on page C10-437</i>
TRCSYNCPR	RW	<i>C10.11 Synchronization Period Register on page C10-438</i>
TRCCCCTLR	RW	<i>C10.12 Cycle Count Control Register on page C10-439</i>
TRCBBCTLR	RW	<i>C10.5 Branch Broadcast Control Register on page C10-430</i>
TRCTRACEIDR	RW	<i>C10.13 Trace ID Register on page C10-440</i>
TRCVICTLR	RW	<i>C10.14 ViewInst Main Control Register on page C10-441</i>
TRCVIIECTLR	RW	<i>C10.15 ViewInst Include-Exclude Control Register on page C10-443</i>
TRCVISSCTLR	RW	<i>C10.16 ViewInst Start-Stop Control Register on page C10-444</i>
TRCSEQEVR0	RW	<i>C10.17 Sequencer State Transition Control Registers 0-2 on page C10-445</i>
TRCSEQEVR1	RW	<i>C10.17 Sequencer State Transition Control Registers 0-2 on page C10-445</i>
TRCSEQEVR2	RW	<i>C10.17 Sequencer State Transition Control Registers 0-2 on page C10-445</i>
TRCSEQRSTEVN	RW	<i>C10.18 Sequencer Reset Control Register on page C10-447</i>
TRCSEQSTR	RW	<i>C10.19 Sequencer State Register on page C10-448</i>
TRCEXTINSELN	RW	<i>C10.20 External Input Select Register on page C10-449</i>
TRCCNTRLDVRO	RW	<i>C10.21 Counter Reload Value Registers 0-1 on page C10-450</i>
TRCCNTRLDVR1	RW	<i>C10.21 Counter Reload Value Registers 0-1 on page C10-450</i>
TRCCNTCTLR0	RW	<i>C10.22 Counter Control Register 0 on page C10-451</i>
TRCCNTCTLR1	RW	<i>C10.23 Counter Control Register 1 on page C10-452</i>
TRCCNTVRO	RW	<i>C10.24 Counter Value Registers 0-1 on page C10-454</i>
TRCCNTVR1	RW	<i>C10.24 Counter Value Registers 0-1 on page C10-454</i>
TRCIDR8	RO	<i>C10.25 ID Register 8 on page C10-455</i>
TRCIDR9	RO	<i>C10.26 ID Register 9 on page C10-456</i>

Table C10-1 ETM trace unit register summary (continued)

Name	Type	Description
TRCIDR10	RO	<i>C10.27 ID Register 10 on page C10-457</i>
TRCIDR11	RO	<i>C10.28 ID Register 11 on page C10-458</i>
TRCIDR12	RO	<i>C10.29 ID Register 12 on page C10-459</i>
TRCIDR13	RO	<i>C10.30 ID Register 13 on page C10-460</i>
TCRIMSPEC0	RW	<i>C10.31 Implementation Specific Register 0 on page C10-461</i>
TRCIDR0	RO	<i>C10.32 ID Register 0 on page C10-462</i>
TRCIDR1	RO	<i>C10.33 ID Register 1 on page C10-464</i>
TRCIDR2	RO	<i>C10.34 ID Register 2 on page C10-465</i>
TRCIDR3	RO	<i>C10.35 ID Register 3 on page C10-466</i>
TRCIDR4	RO	<i>C10.36 ID Register 4 on page C10-468</i>
TRCIDR5	RO	<i>C10.37 ID Register 5 on page C10-469</i>
TRCRSCTLRn	RW	<i>C10.38 Resource Selection Control Registers 2-16 on page C10-471, n is 2, 15</i>
TRCSSCCR0	RW	<i>C10.39 Single-Shot Comparator Control Register 0 on page C10-472</i>
TRCSSCSR0	RW, RO	<i>C10.40 Single-Shot Comparator Status Register 0 on page C10-473</i>
TRCOSLAR	WO	<i>C10.41 OS Lock Access Register on page C10-474</i>
TRCOSLSR	RO	<i>C10.42 OS Lock Status Register on page C10-475</i>
TRCPDCR	RW	<i>C10.43 Power Down Control Register on page C10-476</i>
TRCPDSR	RO	<i>C10.44 Power Down Status Register on page C10-477</i>
TRCACVRn	RW	<i>C10.45 Address Comparator Value Registers 0-7 on page C10-478</i>
TRCACATRn	RW	<i>C10.46 Address Comparator Access Type Registers 0-7 on page C10-479></i>
TRCCIDCVR0	RW	<i>C10.47 Context ID Comparator Value Register 0 on page C10-481</i>
TRCVMIDCVR0	RW	<i>C10.48 VMID Comparator Value Register 0 on page C10-482</i>
TRCCIDCCTLR0	RW	<i>C10.49 Context ID Comparator Control Register 0 on page C10-483</i>
TRCITATBIDR	RW	<i>C10.50 Integration ATB Identification Register on page C10-484</i>
TRCITIDATAR	WO	<i>C10.51 Integration Instruction ATB Data Register on page C10-485</i>
TRCITIATBINR	RO	<i>C10.52 Integration Instruction ATB In Register on page C10-486</i>
TRCITIATBOUTr	WO	<i>C10.53 Integration Instruction ATB Out Register on page C10-487</i>
TRCITCTRL	RW	<i>C10.54 Integration Mode Control Register on page C10-488</i>
TRCCLAIMSET	RW	<i>C10.55 Claim Tag Set Register on page C10-489</i>
TRCCLAIMCLR	RW	<i>C10.56 Claim Tag Clear Register on page C10-490</i>
TRCDEVAFF0	RO	<i>C10.57 Device Affinity Register 0 on page C10-491</i>
TRCDEVAFF1	RO	<i>C10.58 Device Affinity Register 1 on page C10-493</i>
TRCLAR	WO	<i>C10.59 Software Lock Access Register on page C10-494</i>
TRCLSR	RO	<i>C10.60 Software Lock Status Register on page C10-495</i>
TRCAUTHSTATUS	RO	<i>C10.61 Authentication Status Register on page C10-496</i>

Table C10-1 ETM trace unit register summary (continued)

Name	Type	Description
TRCDEVARCH	RO	<i>C10.62 Device Architecture Register on page C10-497</i>
TRCDEVID	RO	<i>C10.63 Device ID Register on page C10-498</i>
TRCDEVTYPE	RO	<i>C10.64 Device Type Register on page C10-499</i>
TRCPIDR4	RO	<i>C10.70 ETM Peripheral Identification Register 4 on page C10-505</i>
TRCPIDR5	RO	<i>C10.71 ETM Peripheral Identification Register 5-7 on page C10-506</i>
TRCPIDR6	RO	
TRCPIDR7	RO	
TRCPIDR0	RO	<i>C10.66 ETM Peripheral Identification Register 0 on page C10-501</i>
TRCPIDR1	RO	<i>C10.67 ETM Peripheral Identification Register 1 on page C10-502</i>
TRCPIDR2	RO	<i>C10.68 ETM Peripheral Identification Register 2 on page C10-503</i>
TRCPIDR3	RO	<i>C10.69 ETM Peripheral Identification Register 3 on page C10-504</i>
TRCCIDR0	RO	<i>C10.73 ETM Component Identification Register 0 on page C10-508</i>
TRCCIDR1	RO	<i>C10.74 ETM Component Identification Register 1 on page C10-509</i>
TRCCIDR2	RO	<i>C10.75 ETM Component Identification Register 2 on page C10-510</i>
TRCCIDR3	RO	<i>C10.76 ETM Component Identification Register 3 on page C10-511</i>

C10.2 Programming Control Register

The TRCPRGCTLR characteristics are:

Purpose

Enables the ETM trace unit.

Usage constraints

See [C3.4 Programming and reading ETM trace unit registers](#) on page C3-321.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary](#) on page C10-423.

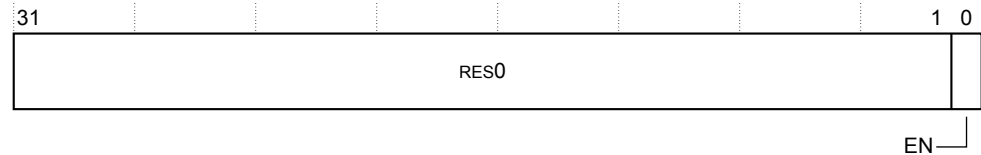


Figure C10-1 TRCPRGCTLR bit assignments

[31:1]

Reserved, RES0.

EN, [0]

Trace program enable:

- 0 The ETM trace unit interface in the processor is disabled, and clocks are enabled only when necessary to process APB accesses, or drain any already generated trace. This is the reset value.
- 1 The ETM trace unit interface in the processor is enabled, and clocks are enabled. Writes to most trace registers are ignored.

The TRCPRGCTLR can be accessed through the external debug interface, offset 0x004.

C10.3 Status Register

The TRCSTATR characteristics are:

Purpose

Indicates the ETM trace unit status.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See *C10.1 ETM register summary* on page C10-423.

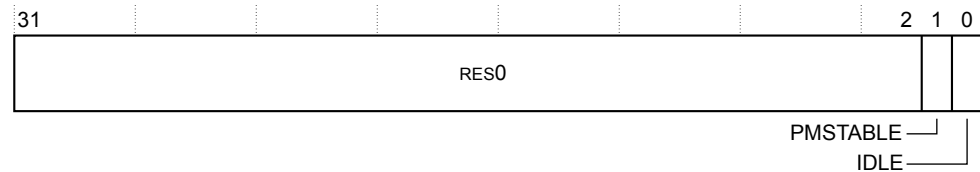


Figure C10-2 TRCSTATR bit assignments

[31:2]

Reserved, RES0.

PMSTABLE, [1]

Indicates whether the ETM trace unit registers are stable and can be read:

- 0 The programmers model is not stable.
- 1 The programmers model is stable.

IDLE, [0]

Idle status:

- 0 The ETM trace unit is not idle.
- 1 The ETM trace unit is idle.

The TRCSTATR can be accessed through the external debug interface, offset 0x00C.

C10.4 Trace Configuration Register

The TRCCONFIGR characteristics are:

Purpose

Controls the tracing options.

Usage constraints

- This register must always be programmed as part of trace unit initialization.
- Only accepts writes when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

TRCCONFIGR is a 32-bit RW trace register.

See [C10.1 ETM register summary on page C10-423](#).

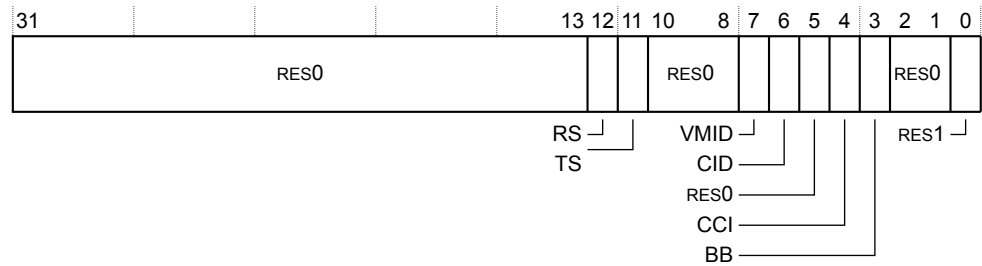


Figure C10-3 TRCCONFIGR bit assignments

[31:13]

Reserved, RES0.

RS, [12]

Enables the return stack. The possible values are:

- 0 Disables the return stack.
- 1 Enables the return stack.

TS, [11]

Enables global timestamp tracing. The possible values are:

- 0 Disables global timestamp tracing.
- 1 Enables global timestamp tracing.

[10:8]

Reserved, RES0.

VMID, [7]

Enables VMID tracing. The possible values are:

- 0 Disables VMID tracing.
- 1 Enables VMID tracing.

CID, [6]

Enables context ID tracing. The possible values are:

- 0 Disables context ID tracing.
- 1 Enables context ID tracing.

[5]

Reserved, RES0.

CCI, [4]

Enables cycle counting instruction trace. The possible values are:

- 0 Disables cycle counting instruction trace.
- 1 Enables cycle counting instruction trace.

BB, [3]

Enables branch broadcast mode. The possible values are:

- 0 Disables branch broadcast mode.
- 1 Enables branch broadcast mode.

[2:1]

Reserved, RES0.

[0]

Reserved, RES1.

The TRCCONFIGR can be accessed through the external debug interface, offset 0x010.

C10.5 Branch Broadcast Control Register

The TRCBBCTLR characteristics are:

Purpose

Controls how branch broadcasting behaves, and enables branch broadcasting to be enabled for certain memory regions.

Usage constraints

- Only accepts writes when the trace unit is disabled.
- Must be programmed if TRCCONFIGR.BB == 1.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

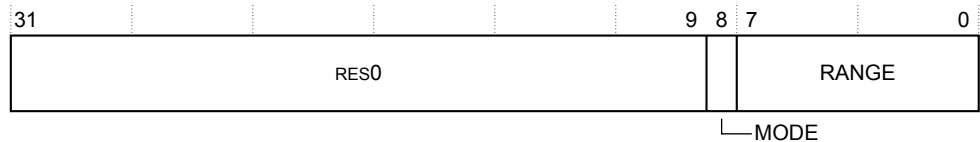


Figure C10-4 TRCBBCTLR bit assignments

[31:9]

Reserved, RES0.

MODE, [8]

Mode bit:

- 0 Exclude mode. Branch broadcasting is not enabled in the address range that RANGE defines.
If RANGE==0 then branch broadcasting is enabled for the entire memory map.
- 1 Include mode. Branch broadcasting is enabled in the address range that RANGE defines.
If RANGE==0 then the behavior of the trace unit is constrained UNPREDICTABLE. That is, the trace unit might or might not consider any instructions to be in a branch broadcast region.

RANGE, [7:0]

Address range field.

Selects which address range comparator pairs are in use with branch broadcasting. Each bit represents an address range comparator pair, so bit[*n*] controls the selection of address range comparator pair *n*. If bit[*n*] is:

- 0 The address range that address range comparator pair *n* defines, is not selected.
- 1 The address range that address range comparator pair *n* defines, is selected.

The TRCBBCTLR can be accessed through the external debug interface, offset 0x03C.

C10.6 Auxiliary Control Register

The TRCAUXCTLR characteristics are:

Purpose

The function of this register is to provide IMPLEMENTATION DEFINED configuration and control options.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

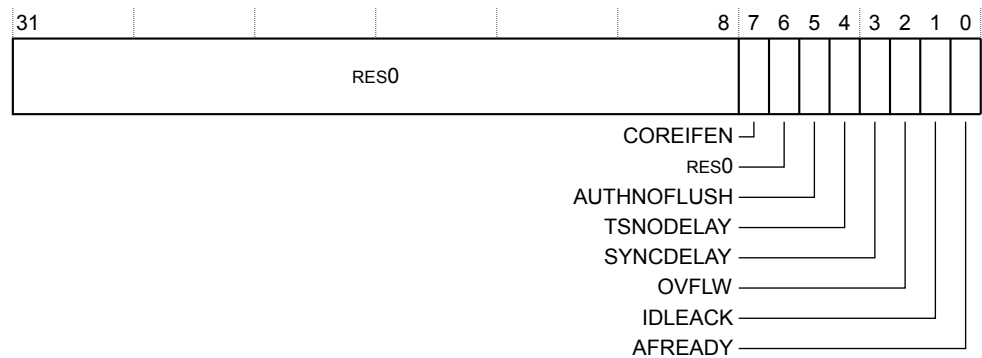


Figure C10-5 TRCAUXCTLR bit assignments

[31:8]

Reserved, RES0.

COREIFEN, [7]

Keep core interface enabled regardless of trace enable register state. The possible values are:

- 0 Core interface enabled is set by trace enable register state.
- 1 Enable core interface, regardless of trace enable register state.

[6]

Reserved, RES0.

AUTHNOFLUSH, [5]

Do not flush trace on de-assertion of authentication inputs. The possible values are:

- 0 ETM trace unit FIFO is flushed and ETM trace unit enters idle state when **DBGEN** or **NIDEN** is LOW.
- 1 ETM trace unit FIFO is not flushed and ETM trace unit does not enter idle state when **DBGEN** or **NIDEN** is LOW.

When this bit is set to 1, the trace unit behavior deviates from architecturally-specified behavior.

TSNODELAY, [4]

Do not delay timestamp insertion based on FIFO depth. The possible values are:

- 0 Timestamp packets are inserted into FIFO only when trace activity is LOW.
- 1 Timestamp packets are inserted into FIFO irrespective of trace activity.

SYNCDELAY, [3]

Delay periodic synchronization if FIFO is more than half-full. The possible values are:

- 0 SYNC packets are inserted into FIFO only when trace activity is low.
- 1 SYNC packets are inserted into FIFO irrespective of trace activity.

OVFLW, [2]

Force overflow if synchronization is not completed when second synchronization becomes due. The possible values are:

- 0 No FIFO overflow when SYNC packets are delayed.
- 1 Forces FIFO overflow when SYNC packets are delayed.

When this bit is set to 1, the trace unit behavior deviates from architecturally-specified behavior.

IDLEACK, [1]

Force idle-drain acknowledge high, CPU does not wait for trace to drain before entering WFX state. The possible values are:

- 0 ETM trace unit idle acknowledge is asserted only when the ETM trace unit is in idle state.
- 1 ETM trace unit idle acknowledge is asserted irrespective of the ETM trace unit idle state.

When this bit is set to 1, trace unit behavior deviates from architecturally-specified behavior.

AFREADY, [0]

Always respond to AFREADY immediately. Does not have any interaction with FIFO draining, even in WFI state. The possible values are:

- 0 ETM trace unit **AFREADYM** output is asserted only when the ETM trace unit is in idle state or when all the trace bytes in FIFO before a flush request are output.
- 1 ETM trace unit **AFREADYM** output is always asserted HIGH. When this bit is set to 1, trace unit behavior deviates from architecturally-specified behavior.

The TRCAUXCTLR can be accessed through the external debug interface, offset 0x018.

C10.7 Event Control 0 Register

The TRCEVENTCTL0R characteristics are:

Purpose

Controls the tracing of events in the trace stream. The events also drive the external outputs from the ETM trace unit. The events are selected from the Resource Selectors.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

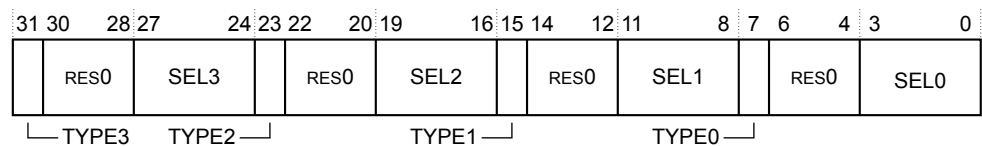


Figure C10-6 TRCEVENTCL0R bit assignments

TYPE3, [31]

Selects the resource type for trace event 3:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[30:28]

Reserved, RES0.

SEL3, [27:24]

Selects the resource number, based on the value of TYPE3:

When TYPE3 is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When TYPE3 is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

TYPE2, [23]

Selects the resource type for trace event 2:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[22:20]

Reserved, RES0.

SEL2, [19:16]

Selects the resource number, based on the value of TYPE2:

When TYPE2 is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When TYPE2 is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

TYPE1, [15]

Selects the resource type for trace event 1:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[14:12]

Reserved, RES0.

SEL1, [11:8]

Selects the resource number, based on the value of TYPE1:

When TYPE1 is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When TYPE1 is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

TYPE0, [7]

Selects the resource type for trace event 0:

0 Single selected resource.

1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

SEL0, [3:0]

Selects the resource number, based on the value of TYPE0:

When TYPE0 is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When TYPE0 is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCEVENTCTL0R can be accessed through the external debug interface, offset 0x020.

C10.8 Event Control 1 Register

The TRCEVENTCTL1R characteristics are:

Purpose

Controls the behavior of the events that TRCEVENTCTL0R selects.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

TRCEVENTCTL1R is a 32-bit RW trace register.

See *C10.1 ETM register summary on page C10-423*.

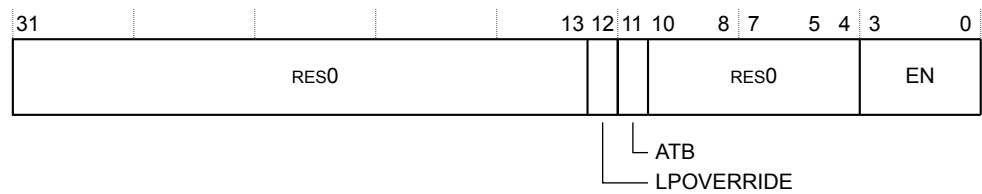


Figure C10-7 TRCEVENTCL1R bit assignments

[31:13]

Reserved, RES0.

LPOVERRIDE, [12]

Low-power state behavior override:

- 0 Low-power state behavior unaffected.
- 1 Low-power state behavior overridden. The resources and Event trace generation are unaffected by entry to a low-power state.

ATB, [11]

ATB trigger enable:

- 0 ATB trigger disabled.
- 1 ATB trigger enabled.

[10:4]

Reserved, RES0.

EN, [3:0]

One bit per event, to enable generation of an event element in the instruction trace stream when the selected event occurs:

- 0 Event does not cause an event element.
- 1 Event causes an event element.

The TRCEVENTCTL1R can be accessed through the external debug interface, offset 0x024.

C10.9 Stall Control Register

The TRCSTALLCTLR characteristics are:

Purpose

Enables the ETM trace unit to stall the Cortex-A34 processor if the ETM trace unit FIFO overflows.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary](#) on page C10-423.

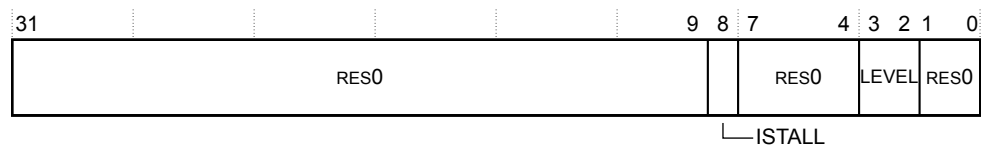


Figure C10-8 TRCSTALLCTLR bit assignments

[31:9]

Reserved, RES0.

ISTALL, [8]

Instruction stall bit. Controls if the trace unit can stall the processor when the instruction trace buffer space is less than LEVEL:

- 0 The trace unit does not stall the processor.
- 1 The trace unit can stall the processor.

[7:4]

Reserved, RES0.

LEVEL, [3:2]

Threshold level field. The field can support 4 monotonic levels from 0b00 to 0b11, where:

- 0b00 Zero invasion. This setting has a greater risk of an ETM trace unit FIFO overflow.
- 0b11 Maximum invasion occurs but there is less risk of a FIFO overflow.

[1:0]

Reserved, RES0.

The TRCSTALLCTLR can be accessed through the external debug interface, offset 0x02c.

C10.10 Global Timestamp Control Register

The TRCTSCTLR characteristics are:

Purpose

Controls the insertion of global timestamps in the trace streams. When the selected event is triggered, the trace unit inserts a global timestamp into the trace streams. The event is selected from one of the Resource Selectors.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- Must be programmed if TRCCONFIGR.TS=1.

Configurations

Available in all configurations.

Attributes

TRCTSCTLR is a 32-bit RW trace register.

The register is set to an UNKNOWN value on a trace unit reset. See also [C10.1 ETM register summary on page C10-423](#).

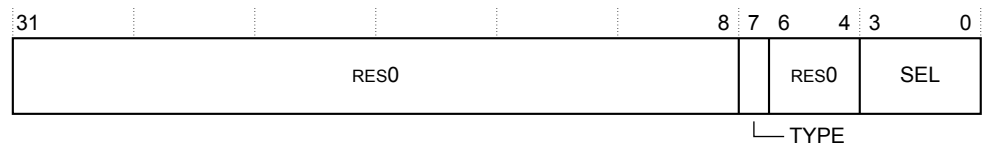


Figure C10-9 TRCTSCTLR bit assignments

[31:8]

Reserved, RES0

TYPE, [7]

Single or combined resource selector.

[6:4]

Reserved.

SEL, [3:1]

Identifies the resource selector to use.

The TRCTSCTLR can be accessed through the external debug interface, offset 0x030.

C10.11 Synchronization Period Register

The TRCSYNCPR characteristics are:

Purpose

Controls how often periodic trace synchronization requests occur.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

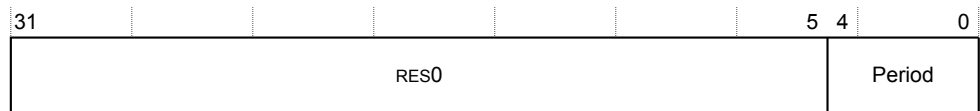


Figure C10-10 TRCSYNCPR bit assignments

[31:5]

Reserved, RES0.

PERIOD, [4:0]

Defines the number of bytes of trace between synchronization requests as a total of the number of bytes generated by both the instruction and data streams. The number of bytes is 2^N where N is the value of this field:

- A value of zero disables these periodic synchronization requests, but does not disable other synchronization requests.
- The minimum value that can be programmed, other than zero, is 8, providing a minimum synchronization period of 256 bytes.
- The maximum value is 20, providing a maximum synchronization period of 2^{20} bytes.

The TRCSYNCPR can be accessed through the external debug interface, offset $0x034$.

C10.12 Cycle Count Control Register

The TRCCCCTLR characteristics are:

Purpose

Sets the threshold value for cycle counting.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- Must be programmed if TRCCONFIGR.CCI==1.
- Minimum value that can be programmed is defined in TRCIDR3.CCITMIN.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

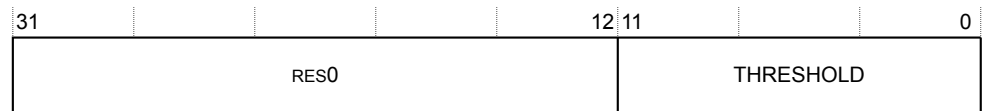


Figure C10-11 TRCCCCTLR bit assignments

[31:12]

Reserved, RES0.

THRESHOLD, [11:0]

Instruction trace cycle count threshold.

The TRCCCCTLR can be accessed through the external debug interface, offset 0x038.

C10.13 Trace ID Register

The TRCTRACEIDR characteristics are:

Purpose

Sets the trace ID for instruction trace.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

TRCTRACEIDR is a 32-bit RW trace register.

See [C10.1 ETM register summary on page C10-423](#).

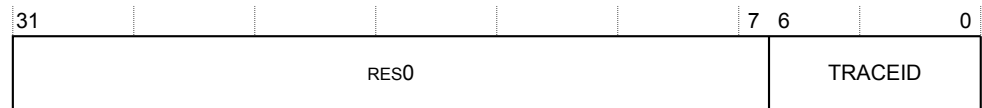


Figure C10-12 TRCTRACEIDR bit Assignments

[31:7]

Reserved, RES0.

TRACEID, [6:0]

Trace ID value. When only instruction tracing is enabled, this provides the trace ID.

The TRCTRACEIDR can be accessed through the external debug interface, offset 0x040.

C10.14 ViewInst Main Control Register

The TRCVICTLR characteristics are:

Purpose

Controls instruction trace filtering.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- Returns stable data only when TRCSTATR.PMSTABLE==1.
- Must be programmed, particularly to set the value of the SSSTATUS bit, that sets the state of the start-stop logic.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

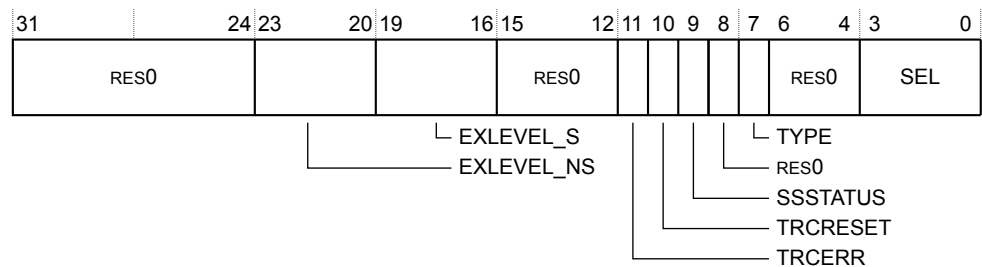


Figure C10-13 TRCVICTLR bit assignments

[31:24]

Reserved, RES0.

EXLEVEL_NS, [23:20]

In Non-secure state, each bit controls whether instruction tracing is enabled for the corresponding exception level:

- 0 Trace unit generates instruction trace, in Non-secure state, for exception level n .
- 1 Trace unit does not generate instruction trace, in Non-secure state, for exception level n .

The exception levels are:

- Bit[20]** Exception level 0.
- Bit[21]** Exception level 1.
- Bit[22]** Exception level 2.
- Bit[23]** RAZ/WI. Instruction tracing is not implemented for exception level 3.

EXLEVEL_S, [19:16]

In Secure state, each bit controls whether instruction tracing is enabled for the corresponding exception level:

- 0 Trace unit generates instruction trace, in Secure state, for exception level n .
- 1 Trace unit does not generate instruction trace, in Secure state, for exception level n .

The exception levels are:

- Bit[16]** Exception level 0.
- Bit[17]** Exception level 1.
- Bit[18]** RAZ/WI. Instruction tracing is not implemented for exception level 2.
- Bit[19]** Exception level 3.

[15:12]

Reserved, RES0.

TRCERR, [11]

Selects whether a system error exception must always be traced:

- 0 System error exception is traced only if the instruction or exception immediately before the system error exception is traced.
- 1 System error exception is always traced regardless of the value of ViewInst.

TRCRESET, [10]

Selects whether a reset exception must always be traced:

- 0 Reset exception is traced only if the instruction or exception immediately before the reset exception is traced.
- 1 Reset exception is always traced regardless of the value of ViewInst.

SSSTATUS, [9]

Indicates the current status of the start/stop logic:

- 0 Start/stop logic is in the stopped state.
- 1 Start/stop logic is in the started state.

[8]

Reserved, RES0.

TYPE, [7]

Selects the resource type for the viewinst event:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

SEL, [3:0]

Selects the resource number to use for the viewinst event, based on the value of TYPE:

When TYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When TYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCVICTLR can be accessed through the external debug interface, offset 0x080.

C10.15 ViewInst Include-Exclude Control Register

The TRCVIIECTLR characteristics are:

Purpose

Defines the address range comparators that control the ViewInst Include/Exclude control.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

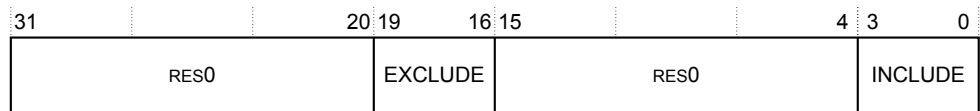


Figure C10-14 TRCVIIECTLR bit assignments

[31:20]

Reserved, RES0.

EXCLUDE, [19:16]

Defines the address range comparators for ViewInst exclude control. One bit is provided for each implemented Address Range Comparator.

[15:4]

Reserved, RES0.

INCLUDE, [3:0]

Defines the address range comparators for ViewInst include control.

Selecting no include comparators indicates that all instructions must be included. The exclude control indicates which ranges must be excluded.

One bit is provided for each implemented Address Range Comparator.

The TRCVIIECTLR can be accessed through the external debug interface, offset `0x084`.

C10.16 ViewInst Start-Stop Control Register

The TRCVISSCTLR characteristics are:

Purpose

Defines the single address comparators that control the ViewInst Start/Stop logic.

Usage constraints

- You must always program this register as part of trace unit initialization.
- Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

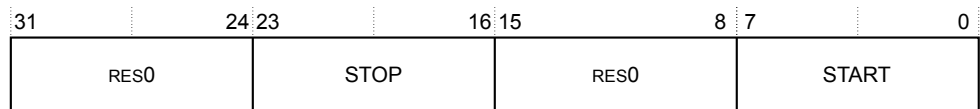


Figure C10-15 TRCVISSCTLR bit assignments

[31:24]

Reserved, RES0.

STOP, [23:16]

Defines the single address comparators to stop trace with the ViewInst Start/Stop control.

One bit is provided for each implemented single address comparator.

[15:8]

Reserved, RES0.

START, [7:0]

Defines the single address comparators to start trace with the ViewInst Start/Stop control.

One bit is provided for each implemented single address comparator.

The TRCVISSCTLR can be accessed through the external debug interface, offset $0x088$.

C10.17 Sequencer State Transition Control Registers 0-2

The TRCSEQEVRn characteristics are:

Purpose

Defines the sequencer transitions that progress to the next state or backwards to the previous state. The ETM trace unit implements a sequencer state machine with up to four states.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- Returns stable data only when TRCSTATR.PMSTABLE==1.
- Software must use this register to set the initial state of the sequencer before the sequencer is used.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

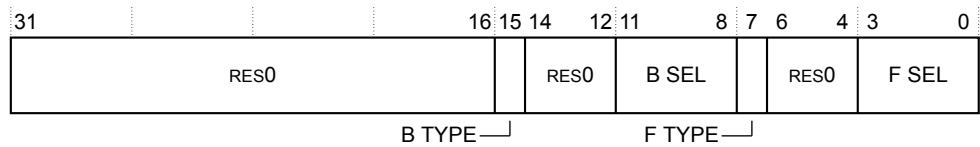


Figure C10-16 TRCSEQEVRn bit assignments

[31:16]

Reserved, RES0.

B TYPE, [15]

Selects the resource type to move backwards to this state from the next state:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[14:12]

Reserved, RES0

B SEL, [11:8]

Selects the resource number, based on the value of B TYPE:

When B TYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When B TYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

F TYPE, [7]

Selects the resource type to move forwards from this state to the next state:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

F SEL, [3:0]

Selects the resource number, based on the value of F TYPE:

When F TYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When F TYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCSEQEVRn registers can be accessed through the external debug interface, offsets:

TRCSEQEVR0

0x100.

TRCSEQVR1
0x104.
TRCSEQVR2
0x108.

C10.18 Sequencer Reset Control Register

The TRCSEQRSTEVr characteristics are:

Purpose

Resets the sequencer to state 0.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- If the sequencer is used, you must program all sequencer state transitions with a valid event.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

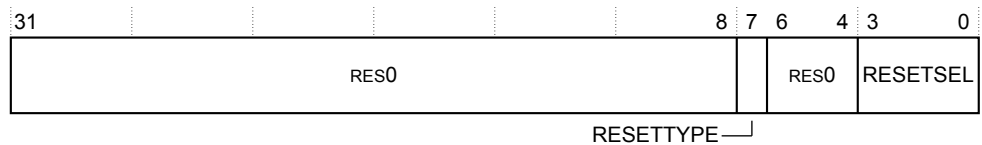


Figure C10-17 TRCSEQRSTEVr bit assignments

[31:8]

Reserved, RES0.

RESETYPE, [7]

Selects the resource type to move back to state 0:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

RESESEL, [3:0]

Selects the resource number, based on the value of RESETYPE:

When RESETYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When RESETYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCSEQRSTEVr can be accessed through the external debug interface, offset 0x118.

C10.19 Sequencer State Register

The TRCSEQSTR characteristics are:

Purpose

Holds the value of the current state of the sequencer.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- Returns stable data only when TRCSTATR.PMSTABLE==1.
- Software must use this register to set the initial state of the sequencer before the sequencer is used.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

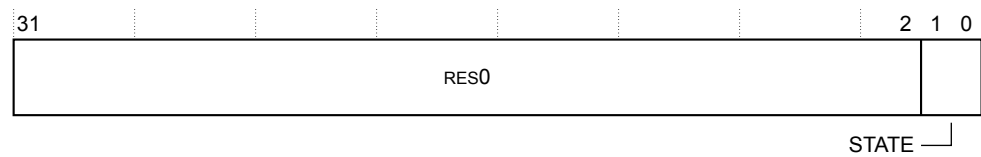


Figure C10-18 TRCSEQSTR bit assignments

[31:2]

Reserved, RES0.

STATE, [1:0]

Current sequencer state:

- 0b00 State 0.
- 0b01 State 1.
- 0b10 State 2.
- 0b11 State 3.

The TRCSEQSTR can be accessed through the external debug interface, offset 0x11c.

C10.20 External Input Select Register

The TRCEXTINSELR characteristics are:

Purpose

Controls the selectors that choose an external input as a resource in the ETM trace unit. You can use the Resource Selectors to access these external input resources.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

31	29	28	24	23	21	20	16	15	13	12	8	7	5	4	0								
RES0			SEL3			RES0			SEL2			RES0			SEL1			RES0			SEL0		

Figure C10-19 TRCEXTINSELR bit assignments

[31:29]

Reserved, RES0.

SEL3, [28:24]

Selects an event from the external input bus for External Input Resource 3.

[23:21]

Reserved, RES0.

SEL2, [20:16]

Selects an event from the external input bus for External Input Resource 2.

[15:13]

Reserved, RES0.

SEL1, [12:8]

Selects an event from the external input bus for External Input Resource 1.

[7:5]

Reserved, RES0.

SEL0, [4:0]

Selects an event from the external input bus for External Input Resource 0.

The TRCEXTINSELR can be accessed through the external debug interface, offset 0x120.

C10.21 Counter Reload Value Registers 0-1

The TRCCNTRLDVRn characteristics are:

Purpose

Defines the reload value for the counter.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

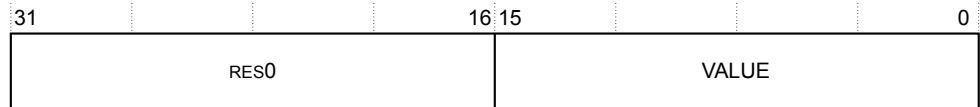


Figure C10-20 TRCCNTRLDVRn bit assignments

[31:16]

Reserved, RES0.

VALUE, [15:0]

Defines the reload value for the counter. This value is loaded into the counter each time the reload event occurs.

The TRCCNTRLDVRn registers can be accessed through the external debug interface, offsets:

TRCCNTRLDVR0

0x140.

TRCCNTRLDVR1

0x144.

C10.22 Counter Control Register 0

The TRCCNTCTLR0 characteristics are:

Purpose

Controls the counter.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

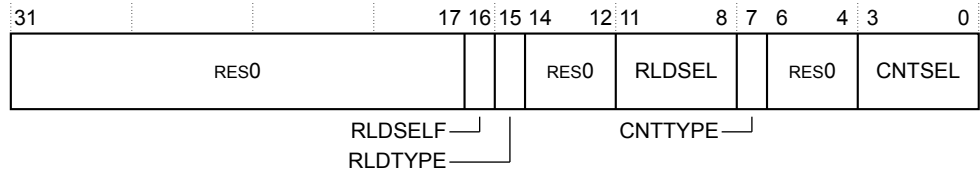


Figure C10-21 TRCCNTCTLR0 bit assignments

[31:17]

Reserved, RES0.

RLDSELF, [16]

Defines whether the counter reloads when it reaches zero:

- 0 The counter does not reload when it reaches zero. The counter only reloads based on RLDTYPE and RLDSEL.
- 1 The counter reloads when it reaches zero and the resource selected by CNTTYPE and CNTSEL is also active. The counter also reloads based on RLDTYPE and RLDSEL.

RLDTYPE, [15]

Selects the resource type for the reload:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[14:12]

Reserved, RES0.

RLDSEL, [11:8]

Selects the resource number, based on the value of RLDTYPE:

When RLDTYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When RLDTYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

CNTTYPE, [7]

Selects the resource type for the counter:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

CNTSEL, [3:0]

Selects the resource number, based on the value of CNTTYPE:

When CNTTYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When CNTTYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCCNTCTLR0 can be accessed through the external debug interface, offset 0x150.

C10.23 Counter Control Register 1

The TRCCNTCTLR1 characteristics are:

Purpose

Controls the counter.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

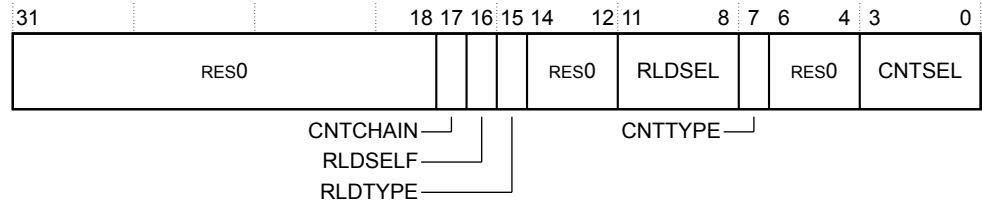


Figure C10-22 TRCCNTCTLR1 bit assignments

[31:18]

Reserved, RES0.

CNTCHAIN, [17]

Defines whether the counter decrements when the counter reloads. This enables two counters to be used in combination to provide a larger counter:

- 0 The counter operates independently from the counter. The counter only decrements based on CNTTYPE and CNTSEL.
- 1 The counter decrements when the counter reloads. The counter also decrements when the resource selected by CNTTYPE and CNTSEL is active.

RLDSELF, [16]

Defines whether the counter reloads when it reaches zero:

- 0 The counter does not reload when it reaches zero. The counter only reloads based on RLDTYPE and RLDSEL.
- 1 The counter reloads when it is zero and the resource selected by CNTTYPE and CNTSEL is also active. The counter also reloads based on RLDTYPE and RLDSEL.

RLDTYPE, [15]

Selects the resource type for the reload:

- 0 Single selected resource.
- 1 Boolean combined resource pair.

[14:12]

Reserved, RES0.

RLDSEL, [11:8]

Selects the resource number, based on the value of RLDTYPE:

When RLDTYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When RLDTYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

CNTTYPE, [7]

Selects the resource type for the counter:

- 0 Single selected resource.

1 Boolean combined resource pair.

[6:4]

Reserved, RES0.

CNTSEL, [3:0]

Selects the resource number, based on the value of CNTTYPE:

When CNTTYPE is 0, selects a single selected resource from 0-15 defined by bits[3:0].

When CNTTYPE is 1, selects a Boolean combined resource pair from 0-7 defined by bits[2:0].

The TRCCNTCTLR1 can be accessed through the external debug interface, offset 0x154.

C10.24 Counter Value Registers 0-1

The TRCCNTVRn characteristics are:

Purpose

Contains the current counter value.

Usage constraints

- Can be written only when the ETM trace unit is disabled.
- The count value is stable only when TRCSTATR.PMSTABLE==1.
- If software uses counter <n>, then it must write to this register to set the initial counter value.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

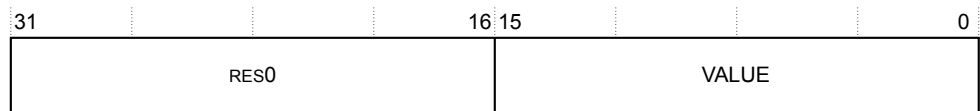


Figure C10-23 TRCCNTVRn bit assignments

[31:16]

Reserved, RES0.

VALUE, [15:0]

Contains the current counter value.

The TRCCNTVRn registers can be accessed through the external debug interface, offsets:

TRCCNTVR0

0x160.

TRCCNTVR1

0x164.

C10.25 ID Register 8

The TRCIDR8 characteristics are:

Purpose

Returns the maximum speculation depth of the instruction trace stream.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

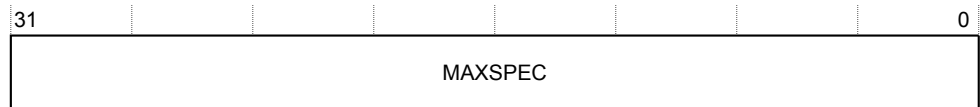


Figure C10-24 TRCIDR8 bit assignments

MAXSPEC, [31:0]

The maximum number of P0 elements in the trace stream that can be speculative at any time.

0 Maximum speculation depth of the instruction trace stream.

The TRCIDR8 can be accessed through the external debug interface, offset 0x180.

C10.26 ID Register 9

The TRCIDR9 characteristics are:

Purpose

Returns the number of P0 right-hand keys that the trace unit can use.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary](#) on page C10-423.

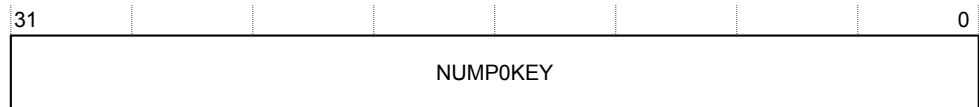


Figure C10-25 TRCIDR9 bit assignments

NUMP0KEY, [31:0]

The number of P0 right-hand keys that the trace unit can use.

0 Number of P0 right-hand keys.

The TRCIDR9 can be accessed through the external debug interface, offset 0x184.

C10.27 ID Register 10

The TRCIDR10 characteristics are:

Purpose

Returns the number of P1 right-hand keys that the trace unit can use.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

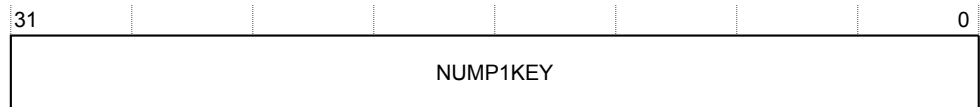


Figure C10-26 TRCIDR10 bit assignments

NUMP1KEY, [31:0]

The number of P1 right-hand keys that the trace unit can use.

0 Number of P1 right-hand keys.

The TRCIDR10 can be accessed through the external debug interface, offset 0x188.

C10.28 ID Register 11

The TRCIDR11 characteristics are:

Purpose

Returns the number of special P1 right-hand keys that the trace unit can use.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

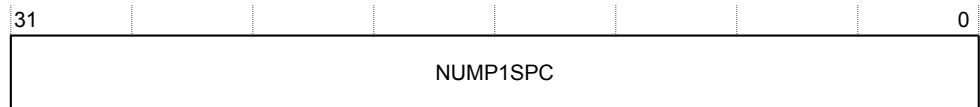


Figure C10-27 TRCIDR11 bit assignments

NUMP1SPC, [31:0]

The number of special P1 right-hand keys that the trace unit can use.

0 Number of special P1 right-hand keys.

The TRCIDR11 can be accessed through the external debug interface, offset 0x18C.

C10.29 ID Register 12

The TRCIDR12 characteristics are:

Purpose

Returns the number of conditional instruction right-hand keys that the trace unit can use.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

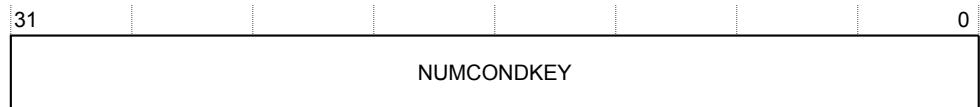


Figure C10-28 TRCIDR12 bit assignments

NUMCONDKEY, [31:0]

The number of conditional instruction right-hand keys that the trace unit can use, including normal and special keys.

0 Number of conditional instruction right-hand keys.

The TRCIDR12 can be accessed through the external debug interface, offset 0x190.

C10.30 ID Register 13

The TRCIDR13 characteristics are:

Purpose

Returns the number of special conditional instruction right-hand keys that the trace unit can use.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

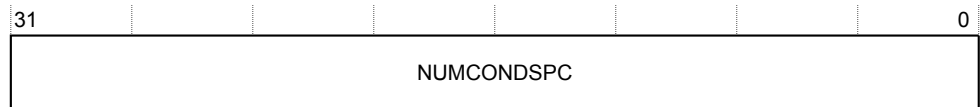


Figure C10-29 TRCIDR13 bit assignments

NUMCONDSPC, [31:0]

The number of special conditional instruction right-hand keys that the trace unit can use, including normal and special keys.

0 Number of special conditional instruction right-hand keys.

The TRCIDR13 can be accessed through the external debug interface, offset 0x194.

C10.31 Implementation Specific Register 0

The TRCIMSPEC0 characteristics are:

Purpose

Shows the presence of any implementation specific features, and enables any features that are provided.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary](#) on page C10-423.

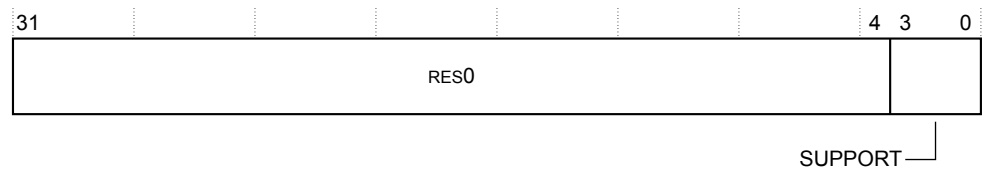


Figure C10-30 TRCIMSPEC0 bit assignments

[31:4]

Reserved, RES0.

SUPPORT, [3:0]

0 No implementation specific extensions are supported.

The TRCIMSPEC0 can be accessed through the external debug interface, offset 0x1C0.

C10.32 ID Register 0

The TRCIDR0 characteristics are:

Purpose

Returns the tracing capabilities of the ETM trace unit.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

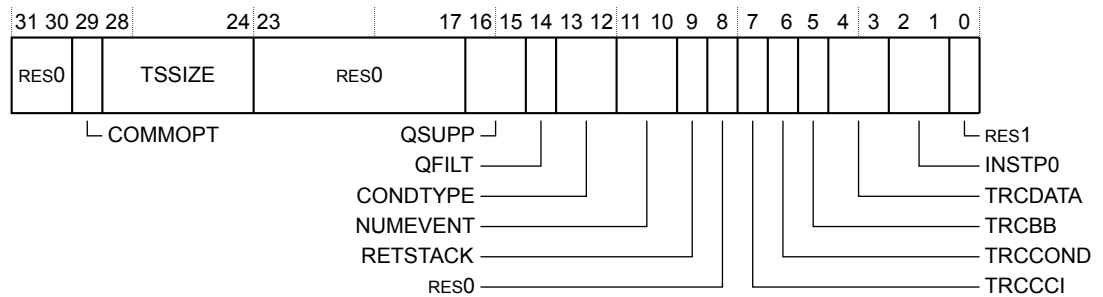


Figure C10-31 TRCIDR0 bit assignments

[31:30]

Reserved, RES0.

COMMOPT, [29]

Indicates the meaning of the commit field in some packets:

1 Commit mode 1.

TSSIZE, [28:24]

Global timestamp size field:

0b01000 Implementation supports a maximum global timestamp of 64 bits.

[23:17]

Reserved, RES0.

QSUPP, [16:15]

Indicates Q element support:

0b00 Q elements not supported.

QFILT, [14]

Indicates Q element filtering support:

0b0 Q element filtering not supported.

CONDTYPE, [13:12]

Indicates how conditional results are traced:

0b00 Conditional trace not supported.

NUMEVENT, [11:10]

Number of events supported in the trace, minus 1:

0b11 Four events supported.

RETSTACK, [9]

Return stack support:

1 Return stack implemented.

[8]

Reserved, RES0.

TRCCCI, [7]

Support for cycle counting in the instruction trace:

1 Cycle counting in the instruction trace is implemented.

TRCCOND, [6]

Support for conditional instruction tracing:

0 Conditional instruction tracing is not supported.

TRCBB, [5]

Support for branch broadcast tracing:

1 Branch broadcast tracing is implemented.

TRCDATA, [4:3]

Conditional tracing field:

0b00 Tracing of data addresses and data values is not implemented.

INSTP0, [2:1]

P0 tracing support field:

0b00 Tracing of load and store instructions as P0 elements is not supported.

[0]

Reserved, RES1.

The TRCIDR0 can be accessed through the external debug interface, offset 0x1E0.

C10.33 ID Register 1

The TRCIDR1 characteristics are:

Purpose

Returns the base architecture of the trace unit.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

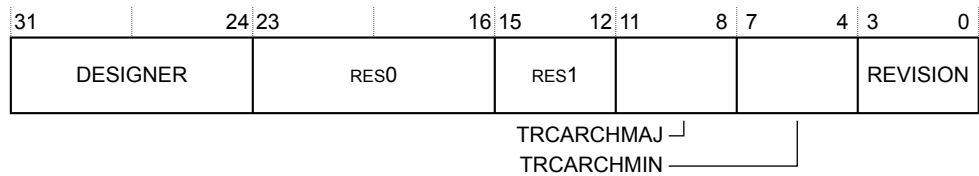


Figure C10-32 TRCIDR1 bit assignments

DESIGNER, [31:24]

Indicates which company designed the trace unit:

0x41 ARM.

[23:16]

Reserved, RES0.

[15:12]

Reserved, RES1.

TRCARCHMAJ, [11:8]

Major trace unit architecture version number:

0b0100 ETMv4.

TRCARCHMIN, [7:4]

Minor trace unit architecture version number:

0b0000 Minor revision 0.

REVISION, [3:0]

Implementation revision number:

0x1 r0p1.

The TRCIDR1 can be accessed through the external debug interface, offset 0x1E4.

C10.34 ID Register 2

The TRCIDR2 characteristics are:

Purpose

Returns the maximum size of the following parameters in the trace unit:

- Cycle counter.
- Data value.
- Data address.
- VMID.
- Context ID.
- Instruction address.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

31	29 28	25 24	20 19	15 14	10 9	5 4	0
RES0	CCSIZE	DVSIZE	DASIZE	VMIDSIZE	CIDSIZE	IASIZE	

Figure C10-33 TRCIDR2 bit assignments

[31:29]

Reserved, RES0.

CCSIZE, [28:25]

Size of the cycle counter in bits minus 12:

0x0 The cycle counter is 12 bits in length.

DVSIZE, [24:20]

Data value size in bytes:

0x00 Data value tracing is not implemented.

DASIZE, [19:15]

Data address size in bytes:

0x00 Data address tracing is not implemented.

VMIDSIZE, [14:10]

Virtual Machine ID size:

0x1 Virtual Machine ID is 8 bits.

CIDSIZE, [9:5]

Context ID size in bytes:

0x4 Maximum of 32-bit Context ID size.

IASIZE, [4:0]

Instruction address size in bytes:

0x8 Maximum of 64-bit address size.

The TRCIDR2 can be accessed through the external debug interface, offset 0x1E8.

TRCERR, [24]

Indicates whether TRCVICTLR.TRCERR is implemented:

1 TRCVICTLR.TRCERR is implemented.

EXLEVEL_NS, [23:20]

Each bit controls whether instruction tracing in Non-secure state is implemented for the corresponding exception level:

0b0111 Instruction tracing is implemented for Non-secure EL0, EL1 and EL2 exception levels.

EXLEVEL_S, [19:16]

Each bit controls whether instruction tracing in Secure state is implemented for the corresponding exception level:

0b1011 Instruction tracing is implemented for Secure EL0, EL1 and EL3 exception levels.

[15:12]

Reserved, RES0.

CCITMIN, [11:0]

The minimum value that can be programmed in TRCCCCTLR.THRESHOLD:

0x004 Instruction trace cycle counting minimum threshold is 4.

The TRCIDR3 can be accessed through the external debug interface, offset 0x1EC.

C10.36 ID Register 4

The TRCIDR4 characteristics are:

Purpose

Indicates the resources available in the ETM trace unit.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

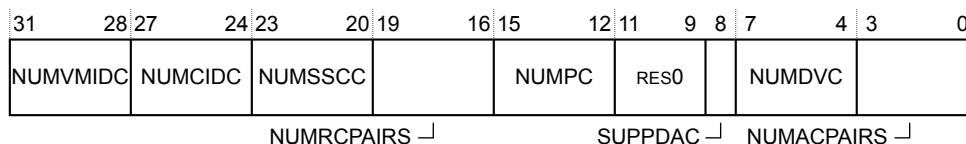


Figure C10-35 TRCIDR4 bit assignments

NUMVMIDC, [31:28]

Indicates the number of VMID comparators available for tracing:

0x1 One VMID comparator is available.

NUMCIDC, [27:24]

Indicates the number of CID comparators available for tracing:

0x1 One Context ID comparator is available.

NUMSSCC, [23:20]

Indicates the number of single-shot comparator controls available for tracing:

0x1 One single-shot comparator control is available.

NUMRSPAIR, [19:16]

Indicates the number of resource selection pairs available for tracing:

0x7 Eight resource selection pairs are available.

NUMPC, [15:12]

Indicates the number of processor comparator inputs available for tracing:

0x0 Processor comparator inputs are not implemented.

[11:9]

Reserved, RES0.

SUPPDAC, [8]

Indicates whether the implementation supports data address comparisons: This value is:

0 Data address comparisons are not implemented.

NUMDVC, [7:4]

Indicates the number of data value comparators available for tracing:

0x0 Data value comparators not implemented.

NUMACPPAIRS, [3:0]

Indicates the number of address comparator pairs available for tracing:

0x4 Four address comparator pairs are implemented.

The TRCIDR4 can be accessed through the external debug interface, offset 0x1F0.

C10.37 ID Register 5

The TRCIDR5 characteristics are:

Purpose

Returns how many resources the trace unit supports.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

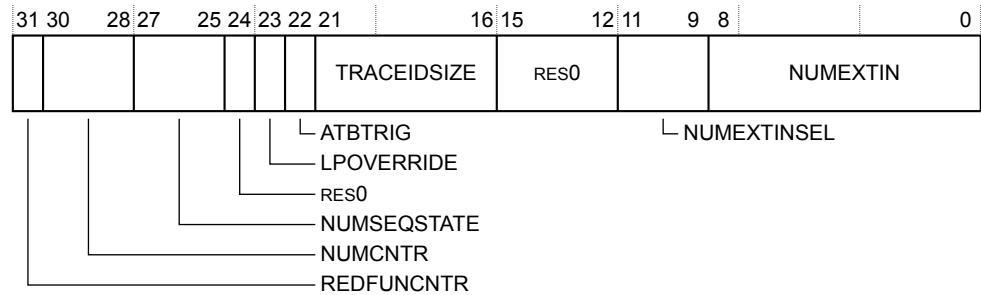


Figure C10-36 TRCIDR5 bit assignments

REDFUNCNTR, [31]

Reduced Function Counter implemented:

0 Reduced Function Counter not implemented.

NUMCCNTR, [30:28]

Number of counters implemented:

0b010 Two counters implemented.

NUMSEQSTATE, [27:25]

Number of sequencer states implemented:

0b100 Four sequencer states implemented.

[24]

Reserved, RES0.

LPOVERRIDE, [23]

Low-power state override support:

1 Low-power state override support implemented.

ATBTRIG, [22]

ATB trigger support:

1 ATB trigger support implemented.

TRACEIDSIZE, [21:16]

Number of bits of trace ID:

0x07 Seven-bit trace ID implemented.

[15:12]

Reserved, RES0.

NUMEXTINSEL, [11:9]

Number of external input selectors implemented:

0b100 Four external input selectors implemented.

NUMEXTIN, [8:0]

Number of external inputs implemented:

0x1E 30 external inputs implemented.

The TRCIDR5 can be accessed through the external debug interface, offset 0x1F4.

C10.38 Resource Selection Control Registers 2-16

The TRCRSCTLRn characteristics are:

Purpose

Controls the trace resources.

There are eight resource pairs, the first pair is predefined as {0,1,pair=0} and having reserved select registers. This leaves seven pairs to be implemented as programmable selectors.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

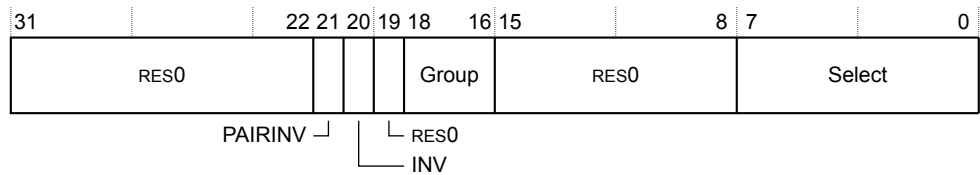


Figure C10-37 TRCRSCTLRn bit assignments

[31:22]

Reserved, RES0.

PAIRINV, [21]

Inverts the result of a combined pair of resources.

This bit is implemented only on the lower register for a pair of resource selectors.

INV, [20]

Inverts the selected resources:

- 0 Resource is not inverted.
- 1 Resource is inverted.

[19]

Reserved, RES0.

GROUP, [18:16]

Selects a group of resources. See the *ARM ETM Architecture Specification, ETMv4* for more information.

[15:8]

Reserved, RES0.

SELECT, [7:0]

Selects one or more resources from the required group. One bit is provided for each resource from the group.

The TRCRSCTLRn can be accessed through the external debug interface, offset 0x208-023C.

C10.39 Single-Shot Comparator Control Register 0

The TRCSSCCR0 characteristics are:

Purpose

Controls the single-shot comparator.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

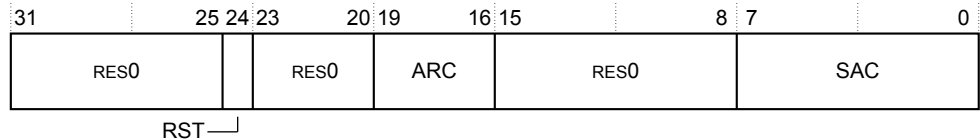


Figure C10-38 TRCSSCCR0 bit assignments

[31:25]

Reserved, RES0.

RST, [24]

Enables the single-shot comparator resource to be reset when it occurs, to enable another comparator match to be detected:

- 1 Reset enabled. Multiple matches can occur.

[23:20]

Reserved, RES0.

ARC, [19:16]

Selects one or more address range comparators for single-shot control.

One bit is provided for each implemented address range comparator.

[15:8]

Reserved, RES0.

SAC, [7:0]

Selects one or more single address comparators for single-shot control.

One bit is provided for each implemented single address comparator.

The TRCSSCCR0 can be accessed through the external debug interface, offset 0x280.

C10.40 Single-Shot Comparator Status Register 0

The TRCSSCSR0 characteristics are:

Purpose

Indicates the status of the single-shot comparator. TRCSSCSR0 is sensitive to instruction addresses.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- The STATUS bit value is stable only when TRCSTATR.PMSTABLE==1.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

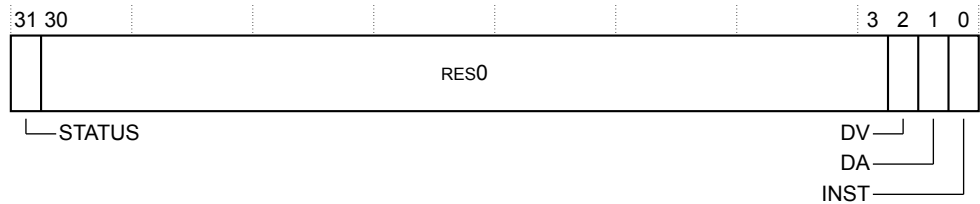


Figure C10-39 TRCSSCSR0 bit assignments

STATUS, [31]

Single-shot status. This indicates whether any of the selected comparators have matched:

- 0 Match has not occurred.
- 1 Match has occurred at least once.

When programming the ETM trace unit, if TRCSSCCRn.RST is b0, the STATUS bit must be explicitly written to 0 to enable this single-shot comparator control.

[30:3]

Reserved, RES0.

DV, [2]

Data value comparator support:

- 0 Single-shot data value comparisons not supported.

DA, [1]

Data address comparator support:

- 0 Single-shot data address comparisons not supported.

INST, [0]

Instruction address comparator support:

- 1 Single-shot instruction address comparisons supported.

The TRCSSCSR0 can be accessed through the external debug interface, offset 0x2A0.

C10.41 OS Lock Access Register

The TRCOSLAR characteristics are:

Purpose

Sets and clears the OS Lock, to lock out external debugger accesses to the ETM trace unit registers.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

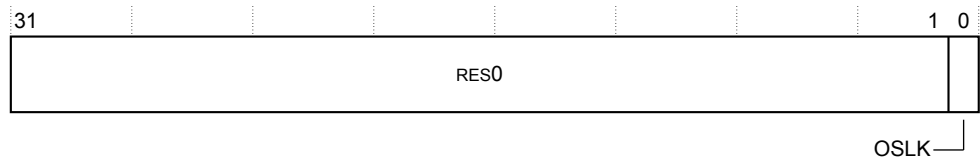


Figure C10-40 TRCOSLAR bit assignments

[31:1]

TRCRSCTLRn

OSLK, [0]

OS Lock key value:

- 0 Unlock the OS Lock.
- 1 Lock the OS Lock.

The TRCOSLAR can be accessed through the external debug interface, offset 0x300.

C10.42 OS Lock Status Register

The TRCOSLSR characteristics are:

Purpose

Returns the status of the OS Lock.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

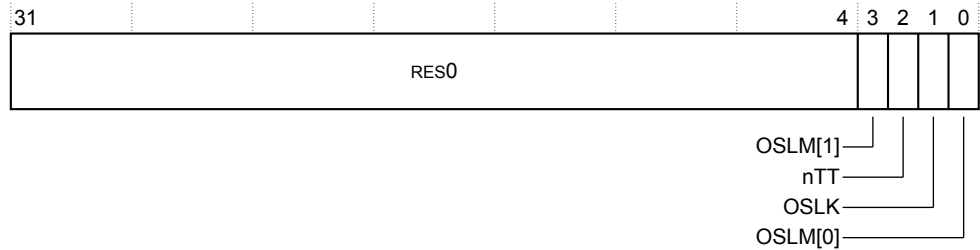


Figure C10-41 TRCOSLSR bit assignments

[31:4]

TRCRSCTRLRN

OSLM[1], [3]

OS Lock model [1] bit. This bit is combined with OSLM[0] to form a two-bit field that indicates the OS Lock model is implemented.

The value of this field is always **0b10**, indicating that the OS Lock is implemented.

nTT, [2]

This bit is RAZ, that indicates that software must perform a 32-bit write to update the TRCOSLAR.

OSLK, [1]

OS Lock status bit:

- 0 OS Lock is unlocked.
- 1 OS Lock is locked.

OSLM[0], [0]

OS Lock model [0] bit. This bit is combined with OSLM[1] to form a two-bit field that indicates the OS Lock model is implemented.

The value of this field is always **0b10**, indicating that the OS Lock is implemented.

The TRCOSLSR can be accessed through the external debug interface, offset **0x304**.

C10.43 Power Down Control Register

The TRCPDCR characteristics are:

Purpose

Request to the system power controller to keep the ETM trace unit powered up.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary](#) on page C10-423.

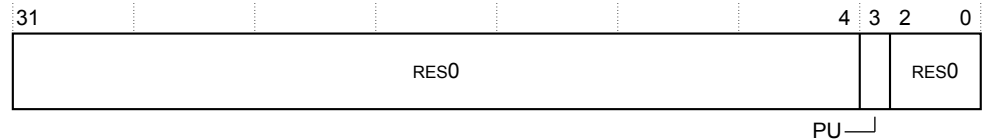


Figure C10-42 TRCPDCR bit assignments

[31:4]

Reserved, RES0.

PU, [3]

Powerup request, to request that power to the ETM trace unit and access to the trace registers is maintained:

- 0 Power not requested.
- 1 Power requested.

This bit is reset to 0 on a trace unit reset.

[2:0]

Reserved, RES0.

The TRCPDCR can be accessed through the external debug interface, offset 0x310.

C10.44 Power Down Status Register

The TRCPDSR characteristics are:

Purpose

Indicates the power down status of the ETM trace unit.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

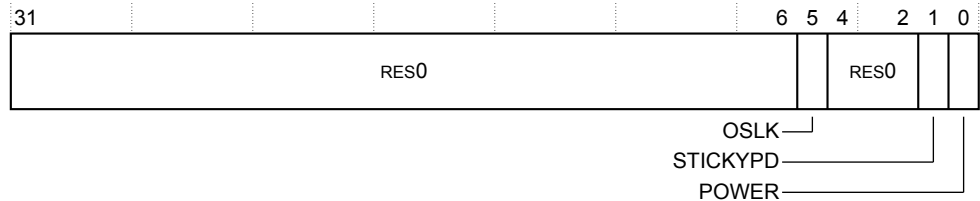


Figure C10-43 TRCPDSR bit assignments

[31:6]

Reserved, RES0.

OSLK, [5]

OS lock status.

- 0 The OS Lock is unlocked.
- 1 The OS Lock is locked.

[4:2]

Reserved, RES0.

STICKYPD, [1]

Sticky power down state.

- 0 Trace register power has not been removed since the TRCPDSR was last read.
- 1 Trace register power has been removed since the TRCPDSR was last read.

This bit is set to 1 when power to the ETM trace unit registers is removed, to indicate that programming state has been lost. It is cleared after a read of the TRCPDSR.

POWER, [0]

Indicates the ETM trace unit is powered:

- 0 ETM trace unit is not powered. The trace registers are not accessible and they all return an error response.
- 1 ETM trace unit is powered. All registers are accessible.

If a system implementation allows the ETM trace unit to be powered off independently of the debug power domain, the system must handle accesses to the ETM trace unit appropriately.

The TRCPDSR can be accessed through the external debug interface, offset 0x314.

C10.45 Address Comparator Value Registers 0-7

The TRCACVRn characteristics are:

Purpose

Indicates the address for the address comparators.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

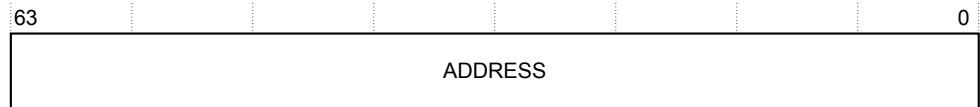


Figure C10-44 TRCACVRn bit assignments

ADDRESS, [63:0]

The address value to compare against.

The TRCACVRn can be accessed through the external debug interface, offset 0x400-0x43C.

C10.46 Address Comparator Access Type Registers 0-7

The TRCACATR_n characteristics are:

Purpose

Controls the access for the corresponding address comparators.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- If software uses two single address comparators as an address range comparator then it must program the corresponding TRCACATR registers with identical values in the following fields:
 - TYPE
 - CONTEXTTYPE
 - EXLEVEL_S
 - EXLEVEL_NS

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

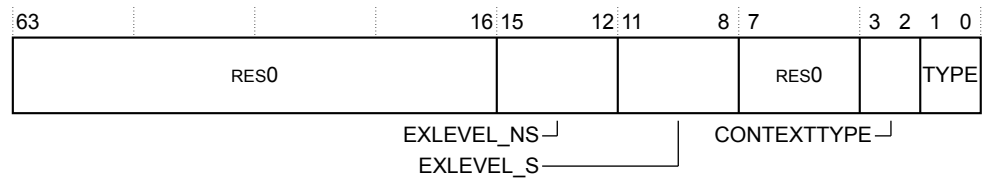


Figure C10-45 TRCACATR_n bit assignments

[63:16]

Reserved, RES0.

EXLEVEL_NS, [15:12]

Each bit controls whether a comparison can occur in Non-secure state for the corresponding exception level. The possible values are:

- 0 The trace unit can perform a comparison, in Non-secure state, for exception level *n*.
- 1 The trace unit does not perform a comparison, in Non-secure state, for exception level *n*.

The exception levels are:

- Bit[12]** Exception level 0.
- Bit[13]** Exception level 1.
- Bit[14]** Exception level 2.
- Bit[15]** Always RES0.

EXLEVEL_S, [11:8]

Each bit controls whether a comparison can occur in Secure state for the corresponding exception level. The possible values are:

- 0 The trace unit can perform a comparison, in Secure state, for exception level *n*.
- 1 The trace unit does not perform a comparison, in Secure state, for exception level *n*.

The exception levels are:

- Bit[8]** Exception level 0.
- Bit[9]** Exception level 1.
- Bit[10]** Always RES0.

Bit[11] Exception level 3.

[7:4]

Reserved, RES0.

Context type, [3:2]

Controls whether the trace unit performs a Context ID comparison, a VMID comparison, or both comparisons:

0b00 The trace unit does not perform a Context ID comparison.

0b01 The trace unit performs a Context ID comparison using the Context ID comparator that the CONTEXT field specifies, and signals a match if both the Context ID comparator matches and the address comparator match.

0b10 The trace unit performs a VMID comparison using the VMID comparator that the CONTEXT field specifies, and signals a match if both the VMID comparator and the address comparator match.

0b11 The trace unit performs a Context ID comparison and a VMID comparison using the comparators that the CONTEXT field specifies, and signals a match if the Context ID comparator matches, the VMID comparator matches, and the address comparator matches.

Type, [1:0]

The type of comparison:

0b00 Instruction address, RES0.

The TRCACATR_n can be accessed through the external debug interface, offset 0x480-0x4B8.

C10.48 VMID Comparator Value Register 0

The TRCVMIDCVR0 characteristics are:

Purpose

Contains a VMID value.

Usage constraints

Accepts writes only when the trace unit is disabled.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

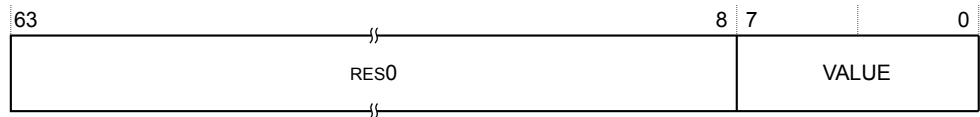


Figure C10-47 TRCVMIDCVR0 bit assignments

[63:8]

Reserved, RES0.

VALUE, [7:0]

The VMID value.

The TRCVMIDCVR0 can be accessed through the external debug interface, offset 0x640.

C10.49 Context ID Comparator Control Register 0

The TRCCIDCCTLR0 characteristics are:

Purpose

Controls the mask value for the context ID comparators.

Usage constraints

- Accepts writes only when the trace unit is disabled.
- If software uses the TRCCIDCVR n registers, where $n=0$ to 3, then it must program this register.
- If software sets a mask bit to 1 then it must program the relevant byte in TRCCIDCVR n to $0x00$.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

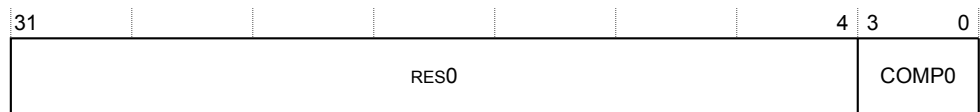


Figure C10-48 TRCCIDCCTLR0 bit assignments

[31:4]

Reserved, RES0.

COMP0, [3:0]

Controls the mask value that the trace unit applies to TRCCIDCVR0. Each bit in this field corresponds to a byte in TRCCIDCVR0. When a bit is:

- 0 The trace unit includes the relevant byte in TRCCIDCVR0 when it performs the Context ID comparison.
- 1 The trace unit ignores the relevant byte in TRCCIDCVR0 when it performs the Context ID comparison.

The TRCCIDCCTLR0 can be accessed through the external debug interface, offset $0x680$.

C10.50 Integration ATB Identification Register

The TRCITATBIDR characteristics are:

Purpose

Sets the state of output pins shown in the following table.

Usage constraints

- Available when bit[0] of TRCITCTRL is set to 1.
- The value of the register sets the signals on the output pins when the register is written.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

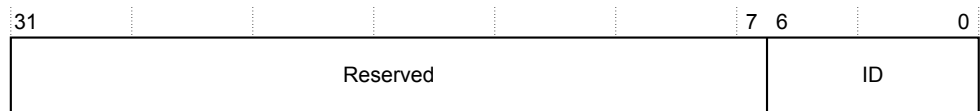


Figure C10-49 TRCITATBIDR bit assignments

[31:7]

Reserved. Read undefined.

ID, [6:0]

Drives the **ATIDMn[6:0]** output pins.

When a bit is set to 0, the corresponding output pin is LOW.

When a bit is set to 1, the corresponding output pin is HIGH.

The TRCITATBIDR bit values correspond to the physical state of the output pins.

The TRCITATBIDR can be accessed through the external debug interface, offset 0xEE4.

C10.51 Integration Instruction ATB Data Register

The TRCITIDATAR characteristics are:

Purpose

Sets the state of the **ATDATAM_n** output pins shown in the following table.

Usage constraints

- Available when bit[0] of TRCITCTRL is set to 1.
- The value of the register sets the signals on the output pins when the register is written.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

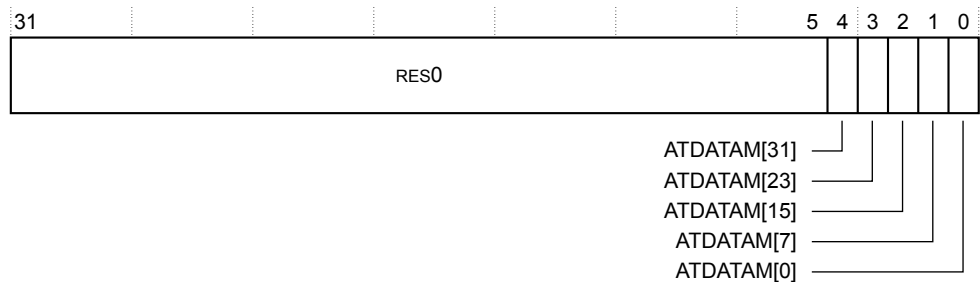


Figure C10-50 TRCITIDATAR bit assignments

For all non-reserved bits:

- When a bit is set to 0, the corresponding output pin is LOW.
- When a bit is set to 1, the corresponding output pin is HIGH.
- The TRCITDDATAR bit values correspond to the physical state of the output pins.

[31:5]

Reserved, RES0.

ATDATAM[31], [4]

Drives the **ATDATAM[31]** output.

ATDATAM[23], [3]

Drives the **ATDATAM[23]** output.

ATDATAM[15], [2]

Drives the **ATDATAM[15]** output.

ATDATAM[7], [1]

Drives the **ATDATAM[7]** output.

ATDATAM[0], [0]

Drives the **ATDATAM[0]** output.

The TRCITIDATAR can be accessed through the external debug interface, offset 0xEEC.

C10.52 Integration Instruction ATB In Register

The TRCITIATBINR characteristics are:

Purpose

Reads the state of the input pins shown in the following table.

Usage constraints

- Available when bit[0] of TRCITCTRL is set to 1.
- The values of the register bits depend on the signals on the input pins when the register is read.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

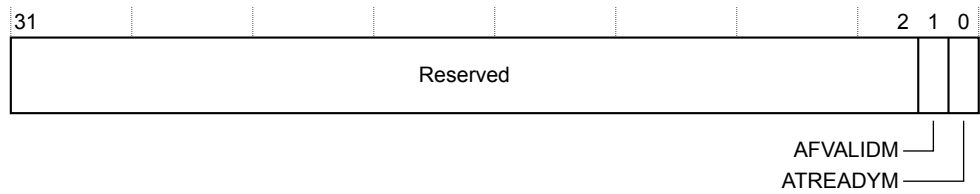


Figure C10-51 TRCITIATBINR bit assignments

For all non-reserved bits:

- When an input pin is LOW, the corresponding register bit is 0.
- When an input pin is HIGH, the corresponding register bit is 1.
- The TRCITIATBINR bit values always correspond to the physical state of the input pins.

[31:2]

Reserved. Read undefined.

AFVALIDM, [1]

Returns the value of the AFVALIDM_n input pin.

ATREADYM, [0]

Returns the value of the ATREADYM_n input pin.

The TRCITIATBINR can be accessed through the external debug interface, offset 0xEF4.

C10.55 Claim Tag Set Register

The TRCCLAIMSET characteristics are:

Purpose

Sets bits in the claim tag and determines the number of claim tag bits implemented.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

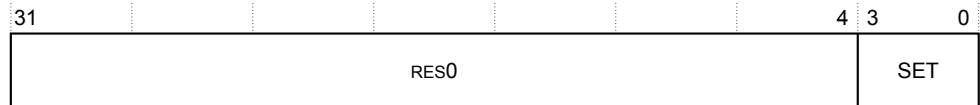


Figure C10-54 TRCCLAIMSET bit assignments

[31:4]

Reserved, RES0.

SET, [3:0]

On reads, for each bit:

- 0 Claim tag bit is not implemented.
- 1 Claim tag bit is implemented.

On writes, for each bit:

- 0 Has no effect.
- 1 Sets the relevant bit of the claim tag.

The TRCCLAIMSET can be accessed through the external debug interface, offset 0xFA0.

C10.56 Claim Tag Clear Register

The TRCCLAIMCLR characteristics are:

Purpose

Clears bits in the claim tag and determines the current value of the claim tag.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

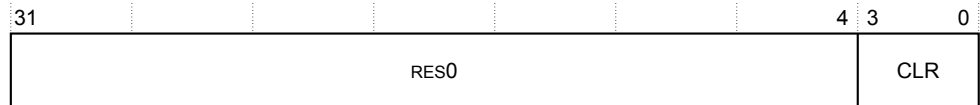


Figure C10-55 TRCCLAIMCLR bit assignments

[31:4]

Reserved, RES0.

CLR, [3:0]

On reads, for each bit:

- 0 Claim tag bit is not set.
- 1 Claim tag bit is set.

On writes, for each bit:

- 0 Has no effect.
- 1 Clears the relevant bit of the claim tag.

The TRCCLAIMCLR can be accessed through the external debug interface, offset 0xFA4.

C10.57 Device Affinity Register 0

The TRCDEVAFF0 characteristics are:

Purpose

Provides an additional core identification mechanism for scheduling purposes in a cluster.

TRCDEVAFF0 is a read-only copy of MPIDR accessible from the external debug interface.

Usage constraints

This register is accessible as follows:

EL0 (NS)	EL0 (S)	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	RO	RO	RO	RO	RO

Configurations

The TRCDEVAFF0 is:

- Architecturally mapped to the AArch64 MPIDR_EL1[31:0] register. See [B1.64 Main ID Register, EL1 on page B1-243](#).
- Architecturally mapped to external TRCDEVAFF0 register.

There is one copy of this register that is used in both Secure and Non-secure states.

Attributes

TRCDEVAFF0 is a 32-bit register.

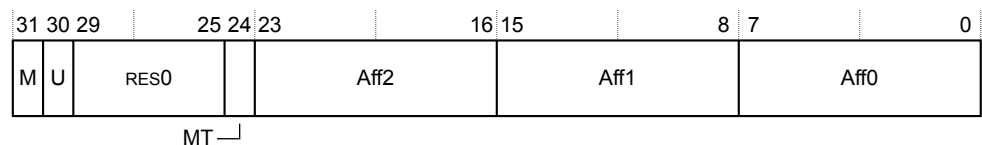


Figure C10-56 TRCDEVAFF0 bit assignments

M, [31]

Reserved, RES1.

U, [30]

Indicates a single core system, as distinct from core 0 in a cluster. This value is:

- 0 Processor is part of a multiprocessor system. This is the value for implementations with more than one core, and for implementations with an ACE or CHI master interface.
- 1 Processor is part of a uniprocessor system. This is the value for single core implementations with an AXI master interface.

[29:25]

Reserved, RES0.

MT, [24]

Indicates whether the lowest level of affinity consists of logical cores that are implemented using a multi-threading type approach. This value is:

- 0 Performance of cores at the lowest affinity level is largely independent.

Aff2, [23:16]

Affinity level 2. Second highest level affinity field.

Indicates the value read in the **CLUSTERIDAFF2** configuration signal.

Aff1, [15:8]

Affinity level 1. Third highest level affinity field.

Indicates the value read in the **CLUSTERIDAFF1** configuration signal.

Aff0, [7:0]

Affinity level 0. Lowest level affinity field.

Indicates the core number in the Cortex-A34 processor. The possible values are:

- 0x0 A processor with one core only.
- 0x0, 0x1 A cluster with two cores.
- 0x0, 0x1, 0x2 A cluster with three cores.
- 0x0, 0x1, 0x2, 0x3 A cluster with four cores.

To access the TRCDEVAFF0:

```
MRC p15,0,<Rt>,c0,c0,5 ; Read TRCDEVAFF0 into Rt
```

Register access is encoded as follows:

Table C10-2 TRCDEVAFF0 access encoding

coproc	opc1	CRn	CRm	opc2
1111	000	0000	0000	101

The TRCDEVAFF0 can be accessed through the external debug interface, offset 0xFA8.

C10.58 Device Affinity Register 1

The TRCDEVAFF1 characteristics are:

Purpose

The value is a read-only copy of MPIDR_EL1[63:32] as seen from EL3, unaffected by VMPIDR_EL2.

Usage constraints

Accessible only from the external debug interface.

Configurations

Available in all configurations.

Attributes

TRCDEVAFF1 is a 32-bit RO management register.

For the Cortex-A34 processor, MPIDR_EL1[63:32] is RES0.

See [C10.1 ETM register summary on page C10-423](#).

The TRCDEVAFF1 can be accessed through the external debug interface, offset 0xFAC.

C10.59 Software Lock Access Register

The TRCLAR characteristics are:

Purpose

Controls access to registers using the memory-mapped interface, when **PADDRDBG31** is LOW.

When the software lock is set, write accesses using the memory-mapped interface to all ETM trace unit registers are ignored, except for write accesses to the TRCLAR.

When the software lock is set, read accesses of TRCPDSR do not change the TRCPDSR.STICKYPD bit. Read accesses of all other registers are not affected.

Usage constraints

Accessible only from the memory-mapped interface.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

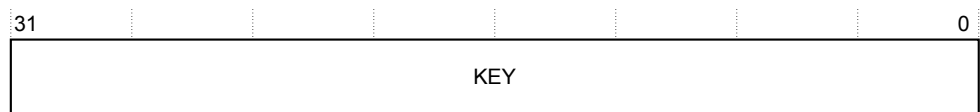


Figure C10-57 TRCLAR bit assignments

KEY, [31:0]

Software lock key value:

0xC5ACCE55 Clear the software lock.

All other write values set the software lock.

The TRCLAR can be accessed through the external debug interface, offset 0xFB0.

C10.60 Software Lock Status Register

The TRCLSR characteristics are:

Purpose

Determines whether the software lock is implemented, and indicates the current status of the software lock.

Usage constraints

Accessible only from the external debug interface.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

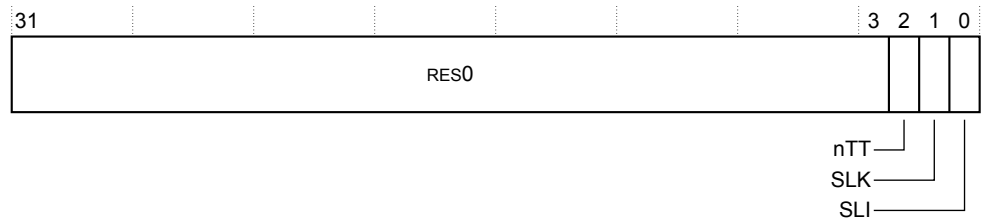


Figure C10-58 TRCLSR bit assignments

[31:3]

Reserved, RES0.

nTT, [2]

Indicates size of TRCLAR:

0 TRCLAR is always 32 bits.

SLK, [1]

Software lock status:

0 Software lock is clear.

1 Software lock is set.

SLI, [0]

Indicates whether the software lock is implemented on this interface.

1 Software lock is implemented on this interface.

The TRCLSR can be accessed through the external debug interface, offset 0xFB4.

C10.61 Authentication Status Register

The TRCAUTHSTATUS characteristics are:

Purpose

Indicates the current level of tracing permitted by the system.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See *C10.1 ETM register summary* on page C10-423.

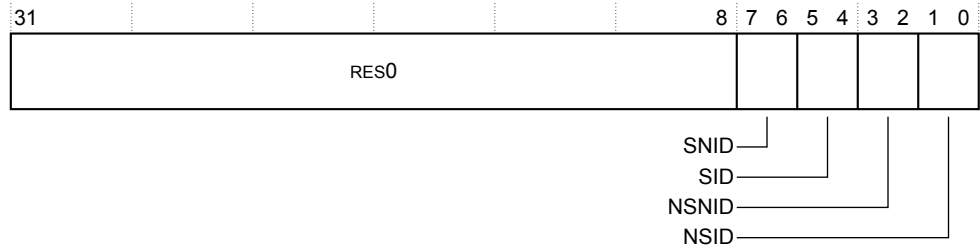


Figure C10-59 TRCAUTHSTATUS bit assignments

[31:8]

Reserved, RES0.

SNID, [7:6]

Secure Non-invasive Debug:

- 0b10 Secure Non-invasive Debug implemented but disabled.
- 0b11 Secure Non-invasive Debug implemented and enabled.

SID, [5:4]

Secure Invasive Debug:

- 0b00 Secure Invasive Debug is not implemented.

NSNID, [3:2]

Non-secure Non-invasive Debug:

- 0b10 Non-secure Non-invasive Debug implemented but disabled, **NIDEN**=0.
- 0b11 Non-secure Non-invasive Debug implemented and enabled, **NIDEN**=1.

NSID, [1:0]

Non-secure Invasive Debug:

- 0b00 Non-secure Invasive Debug is not implemented.

The TRCAUTHSTATUS can be accessed through the external debug interface, offset 0xFB8.

C10.62 Device Architecture Register

The TRCDEVARCH characteristics are:

Purpose

Identifies the ETM trace unit as an ETMv4 component.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

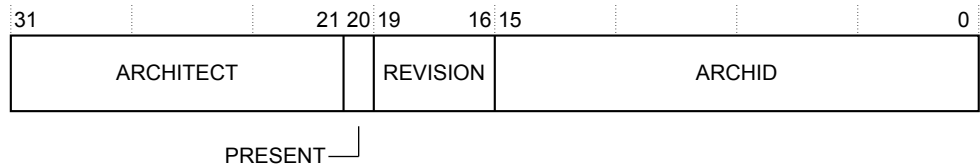


Figure C10-60 TRCDEVARCH bit assignments

ARCHITECT, [31:21]

Defines the architect of the component:

- 0x4 ARM JEP continuation.
- 0x3B ARM JEP 106 code.

PRESENT, [20]

Indicates the presence of this register:

- 0b1 Register is present.

REVISION, [19:16]

Architecture revision:

- 0b0000 Architecture revision 0.

ARCHID, [15:0]

Architecture ID:

- 0x4A13 ETMv4 component.

The TRCDEVARCH can be accessed through the external debug interface, offset 0xFBC.

C10.63 Device ID Register

The TRCDEVID characteristics are:

Purpose

Indicates the capabilities of the ETM trace unit.

Usage constraints

There are no usage constraints.

Configurations

Available in all configurations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

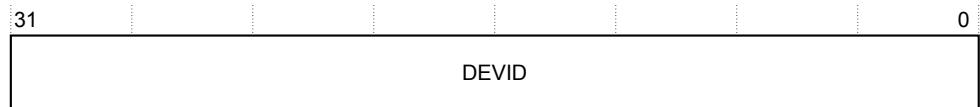


Figure C10-61 TRCDEVID bit assignments

DEVID, [31:0]

RAZ. There are no component-defined capabilities.

The TRCDEVID can be accessed through the external debug interface, offset 0xFC8.

C10.64 Device Type Register

The TRCDEVTYPE characteristics are:

Purpose

Indicates the type of the component.

Usage constraints

Accessible only from the external debug interface.

Configurations

Available in all configurations.

Attributes

C10.1 ETM register summary on page C10-423.



Figure C10-62 TRCDEVTYPE bit assignments

[31:8]

Reserved, RES0.

SUB, [7:4]

The sub-type of the component:

0b0001 Processor trace.

MAJOR, [3:0]

The main type of the component:

0b0011 Trace source.

The TRCDEVTYPE can be accessed through the external debug interface, offset 0xFCC.

C10.65 ETM Peripheral Identification Registers

The ETM Peripheral Identification Registers provide standard information required for all CoreSight components.

The following table lists the Peripheral ID Registers.

Table C10-3 Summary of the Peripheral ID Registers

Register	Value	Offset
Peripheral ID4	0x04	0xFD0
Peripheral ID5	0x00	0xFD4
Peripheral ID6	0x00	0xFD8
Peripheral ID7	0x00	0xFDC
Peripheral ID0	0xDC	0xFE0
Peripheral ID1	0xB9	0xFE4
Peripheral ID2	0x1B	0xFE8
Peripheral ID3	0x00	0xFEC

Only bits[7:0] of each Peripheral ID Register are used, with bits[31:8] reserved. Together, the eight Peripheral ID Registers define a single 64-bit Peripheral ID.

C10.66 ETM Peripheral Identification Register 0

The TRCPIDR0 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debugger interface, offset 0xFE0.

Configurations

Available in all implementations.

Attributes

TRCPIDR0 is a 32-bit RO management register.

See [C10.1 ETM register summary on page C10-423](#).



Figure C10-63 TRCPIDR0 bit assignments

[31:8]

Reserved, RES0.

Part_0, [7:0]

0xDC Least significant byte of the ETM trace unit part number.

C10.67 ETM Peripheral Identification Register 1

The TRCPIDR1 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFE4.

Configurations

Available in all implementations.

Attributes

TRCPIDR1 is a 32-bit RO management register.

See [C10.1 ETM register summary on page C10-423](#).



Figure C10-64 TRCPIDR1 bit assignments

[31:8]

Reserved, RES0.

DES_0, [7:4]

0xB ARM Limited. This is bits[3:0] of JEP106 ID code.

Part_1, [3:0]

0x9 Most significant four bits of the ETM trace unit part number.

C10.68 ETM Peripheral Identification Register 2

The TRCPIDR2 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFE8.

Configurations

Available in all implementations.

Attributes

TRCPIDR2 is a 32-bit RO management register.

See [C10.1 ETM register summary on page C10-423](#).

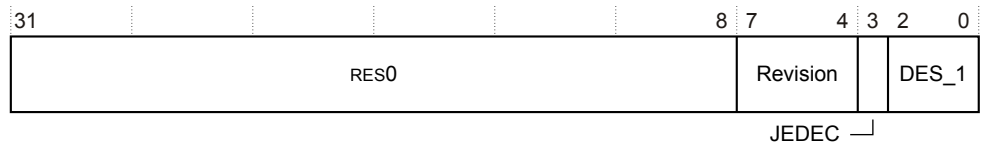


Figure C10-65 TRCPIDR2 bit assignments

[31:8]

Reserved, RES0.

Revision, [7:4]

0x1 r0p1.

JEDEC, [3]

0b1 RES1. Indicates a JEP106 identity code is used.

DES_1, [2:0]

0b011 ARM Limited. This is bits[6:4] of JEP106 ID code.

C10.69 ETM Peripheral Identification Register 3

The TRCPIDR3 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFEC.

Configurations

Available in all implementations.

Attributes

TRCPIDR3 is a 32-bit RO management register.

See [C10.1 ETM register summary on page C10-423](#).



Figure C10-66 TRCPIDR3 bit assignments

[31:8]

Reserved, RES0.

REVAND, [7:4]

0x0 Part minor revision.

CMOD, [3:0]

0x0 Not customer modified.

C10.70 ETM Peripheral Identification Register 4

The TRCPIDR4 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFD0.

Configurations

Available in all implementations.

Attributes

TRCPIDR4 is a 32-bit RO management register.

See [C10.1 ETM register summary on page C10-423](#).



Figure C10-67 TRCPIDR4 bit assignments

[31:8]

Reserved, RES0.

Size, [7:4]

0x0 Size of the component. Log2 the number of 4KB pages from the start of the component to the end of the component ID registers.

DES_2, [3:0]

0x4 ARM Limited. This is bits[3:0] of the JEP106 continuation code.

C10.71 ETM Peripheral Identification Register 5-7

No information is held in the Peripheral ID5, Peripheral ID6, and Peripheral ID7 Registers.
They are reserved for future use and are RES0.

C10.72 ETM Component Identification Registers

There are four read-only ETM Component Identification Registers, Component ID0 to Component ID3.

Table C10-4 Summary of the ETM Component Identification Registers

Register	Value	Offset
Component ID0	0x0D	0xFF0
Component ID1	0x90	0xFF4
Component ID2	0x05	0xFF8
Component ID3	0xB1	0xFFC

The ETM Component Identification Registers identify ETM trace unit as a CoreSight component.

C10.73 ETM Component Identification Register 0

The TRCCIDR0 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFF0.

Configurations

Available in all implementations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

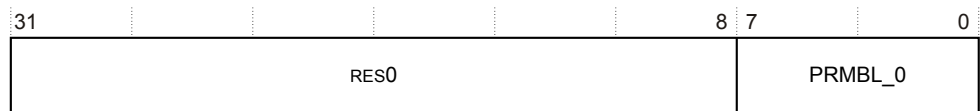


Figure C10-68 TRCCIDR0 bit assignments

[31:8]

Reserved, RES0.

PRMBL_0, [7:0]

0x0D Preamble byte 0.

C10.74 ETM Component Identification Register 1

The TRCCIDR1 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFF4.

Configurations

Available in all implementations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

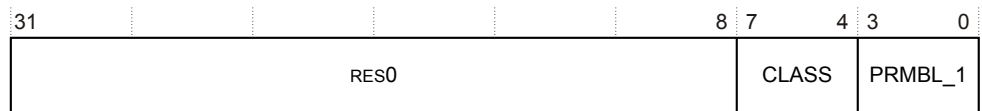


Figure C10-69 TRCCIDR1 bit assignments

[31:8]

Reserved, RES0

CLASS, [7:4]

0x9 Debug component.

PRMBL_1, [3:0]

0x0 Preamble byte 1.

C10.75 ETM Component Identification Register 2

The TRCCIDR2 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFF8.

Configurations

Available in all implementations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

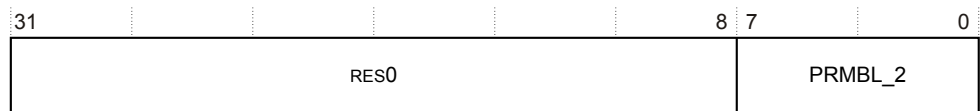


Figure C10-70 TRCCIDR2 bit assignments

[31:8]

Reserved, RES0.

PRMBL_2, [7:0]

0x05 Preamble byte 2.

C10.76 ETM Component Identification Register 3

The TRCCIDR3 characteristics are:

Purpose

Provides information to identify a trace component.

Usage constraints

- Only bits[7:0] are valid.
- Accessible only from the external debug interface, offset 0xFFC.

Configurations

Available in all implementations.

Attributes

See [C10.1 ETM register summary on page C10-423](#).

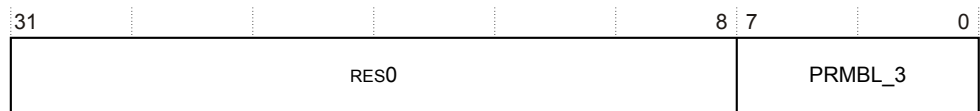


Figure C10-71 TRCCIDR3 bit assignments

[31:8]

Reserved, RES0.

PRMBL_3, [7:0]

0xB1 Preamble byte 3.

Chapter C11

CTI registers

This chapter describes the CTI registers.

It contains the following sections:

- *C11.1 Cross trigger register summary* on page C11-514.
- *C11.2 External register access permissions to the CTI registers* on page C11-516.
- *C11.3 CTI Device Identification Register* on page C11-517.
- *C11.4 CTI Integration Mode Control Register* on page C11-518.
- *C11.5 CTI Peripheral Identification Registers* on page C11-519.
- *C11.6 CTI Peripheral Identification Register 0* on page C11-520.
- *C11.7 CTI Peripheral Identification Register 1* on page C11-521.
- *C11.8 CTI Peripheral Identification Register 2* on page C11-522.
- *C11.9 CTI Peripheral Identification Register 3* on page C11-523.
- *C11.10 CTI Peripheral Identification Register 4* on page C11-524.
- *C11.11 CTI Peripheral Identification Register 5-7* on page C11-525.
- *C11.12 CTI Component Identification Registers* on page C11-526.
- *C11.13 CTI Component Identification Register 0* on page C11-527.
- *C11.14 CTI Component Identification Register 1* on page C11-528.
- *C11.15 CTI Component Identification Register 2* on page C11-529.
- *C11.16 CTI Component Identification Register 3* on page C11-530.

C11.1 Cross trigger register summary

This section describes the cross trigger registers in the Cortex-A34 processor. These registers are accessed through the external debug interface.

The following table gives a summary of the Cortex-A34 cross trigger registers. For those registers not described in this chapter, see the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile*.

Table C11-1 Cross trigger register summary

Offset	Name	Type	Description
0x000	CTICONTROL	RW	CTI Control Register
0x000-0x00C	-	-	Reserved
0x010	CTIINTACK	WO	CTI Output Trigger Acknowledge Register
0x014	CTIAPPSET	RW	CTI Application Trigger Set Register
0x018	CTIAPPCLEAR	WO	CTI Application Trigger Clear Register
0x01C	CTIAPPULSE	WO	CTI Application Pulse Register
0x020	CTIINEN0	RW	CTI Input Trigger to Output Channel Enable Registers
0x024	CTIINEN1	RW	
0x028	CTIINEN2	RW	
0x02C	CTIINEN3	RW	
0x030	CTIINEN4	RW	
0x034	CTIINEN5	RW	
0x038	CTIINEN6	RW	
0x03C	CTIINEN7	RW	
0x040-0x09C	-	-	Reserved
0x0A0	CTIOUTEN0	RW	CTI Input Channel to Output Trigger Enable Registers
0x0A4	CTIOUTEN1	RW	
0x0A8	CTIOUTEN2	RW	
0x0AC	CTIOUTEN3	RW	
0x0B0	CTIOUTEN4	RW	
0x0B4	CTIOUTEN5	RW	
0x0B8	CTIOUTEN6	RW	
0x0BC	CTIOUTEN7	RW	
0x0C0-0x12C	-	-	Reserved
0x130	CTITRIGINSTATUS	RO	CTI Trigger In Status Register
0x134	CTITRIGOUTSTATUS	RO	CTI Trigger Out Status Register
0x138	CTICHINSTATUS	RO	CTI Channel In Status Register
0x13C	CTICHOUTSTATUS	RO	CTI Channel Out Status Register
0x140	CTIGATE	RW	CTI Channel Gate Enable Register

Table C11-1 Cross trigger register summary (continued)

Offset	Name	Type	Description
0x144	ASICCTL	RW	CTI External Multiplexer Control Register
0x148-0xF7C	-	-	Reserved
0xF00	CTIITCTRL	RW	<i>C11.4 CTI Integration Mode Control Register on page C11-518</i>
0xF04-0xFA4	-	-	Reserved
0xFA0	CTICLAIMSET	RW	CTI Claim Tag Set Register
0xFA4	CTICLAIMCLR	RW	CTI Claim Tag Clear Register
0xFA8	CTIDEVAFF0	RO	CTI Device Affinity Register 0
0xFAC	CTIDEVAFF1	RO	CTI Device Affinity Register 1
0xFB0	CTILAR	WO	CTI Lock Access Register
0xFB4	CTILSR	RO	CTI Lock Status Register
0xFB8	CTIAUTHSTATUS	RO	CTI Authentication Status Register
0xFBC	CTIDEVARCH	RO	CTI Device Architecture Register
0xFC0	CTIDEVID2	RO	CTI Device ID Register 2
0xFC4	CTIDEVID1	RO	CTI Device ID Register 1
0xFC8	CTIDEVID	RO	<i>C11.3 CTI Device Identification Register on page C11-517</i>
0xFCC	CTIDEVTYPE	RO	CTI Device Type Register
0xFD0	CTIPIDR4	RO	<i>C11.10 CTI Peripheral Identification Register 4 on page C11-524</i>
0xFD4	CTIPIDR5	RO	<i>C11.11 CTI Peripheral Identification Register 5-7 on page C11-525</i>
0xFD8	CTIPIDR6	RO	
0xFDC	CTIPIDR7	RO	
0xFE0	CTIPIDR0	RO	<i>C11.6 CTI Peripheral Identification Register 0 on page C11-520</i>
0xFE4	CTIPIDR1	RO	<i>C11.7 CTI Peripheral Identification Register 1 on page C11-521</i>
0xFE8	CTIPIDR2	RO	<i>C11.8 CTI Peripheral Identification Register 2 on page C11-522</i>
0xFEC	CTIPIDR3	RO	<i>C11.9 CTI Peripheral Identification Register 3 on page C11-523</i>
0xFF0	CTICIDR0	RO	<i>C11.13 CTI Component Identification Register 0 on page C11-527</i>
0xFF4	CTICIDR1	RO	<i>C11.14 CTI Component Identification Register 1 on page C11-528</i>
0xFF8	CTICIDR2	RO	<i>C11.15 CTI Component Identification Register 2 on page C11-529</i>
0xFFC	CTICIDR3	RO	<i>C11.16 CTI Component Identification Register 3 on page C11-530</i>

C11.2 External register access permissions to the CTI registers

External access permission to the cross trigger registers is subject to the conditions at the time of the access.

The following table describes the processor response to accesses through the external debug and memory-mapped interfaces.

Table C11-2 External register conditions

Name	Condition	Description
Off	EDPRSR.PU is 0	Processor power domain is completely off, or in a low-power state where the processor power domain registers cannot be accessed.
DLK	EDPRSR.DLK is 1	OS Double Lock is locked.
OSLK	OSLSR_EL1.OSLK is 1	OS Lock is locked.
EDAD	AllowExternalDebugAccess() ==FALSE	External debug access is disabled. 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 EDPRSR.SDAD is unchanged.
SLK	Memory-mapped interface only	Software lock is locked. For the external debug interface, ignore this row.
Default	-	None of the conditions apply, normal access.

The following table shows an example of external register condition codes for access to a cross trigger register. To determine the access permission for the register, scan the columns from left to right. Stop at the first column a condition is true, the entry gives the access permission of the register and scanning stops.

Table C11-3 External register condition code example

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	RO/WI	RO

C11.3 CTI Device Identification Register

The CTIDEVID characteristics are:

Purpose

Describes the CTI component to the debugger.

Usage constraints

The accessibility of CTIDEVID by condition code is:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIDEVID is in the Debug power domain.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.

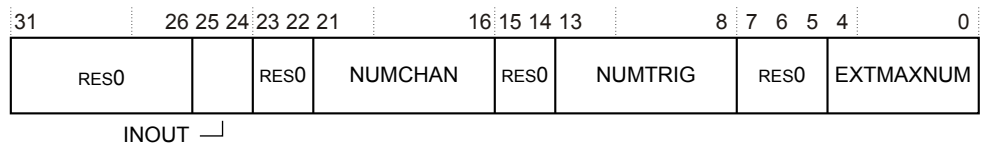


Figure C11-1 CTIDEVID bit assignments

[31:26]

Reserved, RES0.

INOUT, [25:24]

Input and output options. Indicates the presence of an input gate. The possible values are:

- 0b00 CTIGATE does not mask propagation of input events from external channels.
- 0b01 CTIGATE masks propagation of input events from external channels.

[23:22]

Reserved, RES0.

NUMCHAN, [21:16]

Number of channels implemented. This value is:

- 0b00100 Four channels implemented.

[15:14]

Reserved, RES0.

NUMTRIG, [13:8]

Number of triggers implemented. This value is:

- 0b01000 Eight triggers implemented.

[7:5]

Reserved, RES0.

EXTMAXNUM, [4:0]

Maximum number of external triggers implemented. This value is:

- 0b00000 No external triggers implemented.

CTIDEVID can be accessed through the external debug interface, offset 0xFC8.

C11.4 CTI Integration Mode Control Register

The CTIITCTRL characteristics are:

Purpose

The CTIITCTRL shows that the Cortex-A34 processor does not implement an integration mode.

Usage constraints

The accessibility of CTIITCTRL by condition code is:

Off	DLK	OSLK	EDAD	SLK	Default
-	-	-	-	RO/WI	RW

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIITCTRL is in the Debug power domain.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.

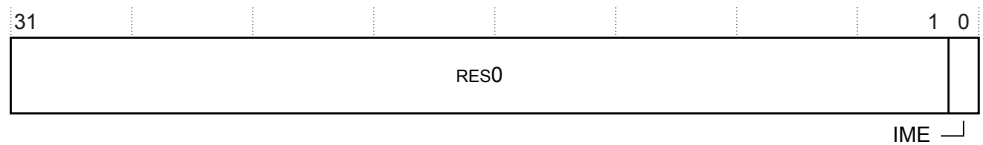


Figure C11-2 CTIITCTRL bit assignments

[31:1]

Reserved, RES0.

IME, [0]

Integration mode enable. The possible value is:

0 Normal operation.

CTIITCTRL can be accessed through the external debug interface, offset 0xF00.

C11.5 CTI Peripheral Identification Registers

The CTI Peripheral Identification Registers provide standard information required for all components that conform to the ARM CoreSight architecture.

The following table lists the CTI Peripheral Identification Registers.

Table C11-4 Summary of the CTI Peripheral Identification Registers

Register	Value	Offset
Peripheral ID4	0x04	0xFD0
Peripheral ID5	0x00	0xFD4
Peripheral ID6	0x00	0xFD8
Peripheral ID7	0x00	0xFDC
Peripheral ID0	0xDC	0xFE0
Peripheral ID1	0xB9	0xFE4
Peripheral ID2	0x1B	0xFE8
Peripheral ID3	0x00	0xFEC

Only bits[7:0] of each Peripheral ID Register are used, with bits[31:8] reserved. Together, the eight Peripheral ID Registers define a single 64-bit Peripheral ID.

C11.6 CTI Peripheral Identification Register 0

The CTIPIDR0 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTIPIDR0 by condition code is:

Off	DLK	OSLK	EPMA	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIPIDR0 is in the Debug power domain.

CTIPIDR0 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-3 CTIPIDR0 bit assignments

[31:8]

Reserved, RES0.

Part_0, [7:0]

0xDC Least significant byte of the cross trigger part number.

CTIPIDR0 can be accessed through the external debug interface, offset 0xFE0.

C11.7 CTI Peripheral Identification Register 1

The CTIPIDR1 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTIPIDR1 by condition code is:

Off	DLK	OSLK	EPAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIPIDR1 is in the Debug power domain.

CTIPIDR1 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-4 CTIPIDR1 bit assignments

[31:8]

Reserved, RES0.

DES_0, [7:4]

0xB ARM Limited. This is the least significant nibble of JEP106 ID code.

Part_1, [3:0]

0x9 Most significant nibble of the CTI part number.

CTIPIDR1 can be accessed through the external debug interface, offset 0xFE4.

C11.8 CTI Peripheral Identification Register 2

The CTIPIDR2 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTIPIDR2 by condition code is:

Off	DLK	OSLK	EPMA	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIPIDR2 is in the Debug power domain.

CTIPIDR2 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.

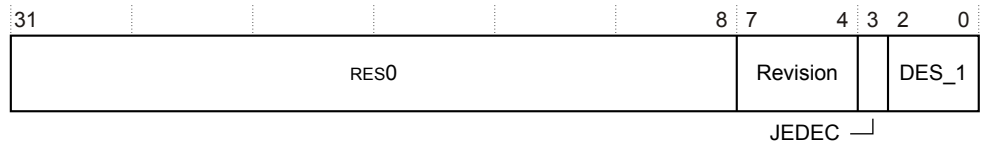


Figure C11-5 CTIPIDR2 bit assignments

[31:8]

Reserved, RES0.

Revision, [7:4]

0x1 r0p1.

JEDEC, [3]

0b1 RES1. Indicates a JEP106 identity code is used.

DES_1, [2:0]

0b011 ARM Limited. This is the most significant nibble of JEP106 ID code.

CTIPIDR2 can be accessed through the external debug interface, offset 0xFE8.

C11.9 CTI Peripheral Identification Register 3

The CTIPIDR3 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTIPIDR3 by condition code is:

Off	DLK	OSLK	EPAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIPIDR3 is in the Debug power domain.

CTIPIDR3 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-6 CTIPIDR3 bit assignments

[31:8]

Reserved, RES0.

REVAND, [7:4]

0x0 Part minor revision.

CMOD, [3:0]

0x0 Customer modified.

CTIPIDR3 can be accessed through the external debug interface, offset 0xFEC.

C11.10 CTI Peripheral Identification Register 4

The CTIPIDR4 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTIPIDR4 by condition code is:

Off	DLK	OSLK	EPMAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTIPIDR4 is in the Debug power domain.

CTIPIDR4 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-7 CTIPIDR4 bit assignments

[31:8]

Reserved, RES0.

Size, [7:4]

0x0 Size of the component. Log2 the number of 4KB pages from the start of the component to the end of the component ID registers.

DES_2, [3:0]

0x4 ARM Limited. This is the least significant nibble JEP106 continuation code.

CTIPIDR4 can be accessed through the external debug interface, offset 0xFD0.

C11.11 CTI Peripheral Identification Register 5-7

No information is held in the Peripheral ID5, Peripheral ID6, and Peripheral ID7 Registers.
They are reserved for future use and are RES0.

C11.12 CTI Component Identification Registers

There are four read-only CTI Component Identification Registers, Component ID0 through Component ID3.

Table C11-5 Summary of the CTI Component Identification Registers

Register	Value	Offset
Component ID0	0x0D	0xFF0
Component ID1	0x90	0xFF4
Component ID2	0x05	0xFF8
Component ID3	0xB1	0xFFC

C11.13 CTI Component Identification Register 0

The CTICIDR0 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTICIDR0 by condition code is:

Off	DLK	OSLK	EPAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTICIDR0 is in the Debug power domain.

CTICIDR0 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-8 CTICIDR0 bit assignments

[31:8]

Reserved, RES0.

PRMBL_0, [7:0]

0x0D Preamble byte 0.

CTICIDR0 can be accessed through the external debug interface, offset 0xFF0.

C11.14 CTI Component Identification Register 1

The CTICIDR1 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTICIDR1 by condition code is:

Off	DLK	OSLK	EPAD	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTICIDR1 is in the Debug power domain.

CTICIDR1 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-9 CTICIDR1 bit assignments

[31:8]

Reserved, RES0.

CLASS, [7:4]

0x9 Debug component.

PRMBL_1, [3:0]

0x0 Preamble byte 1.

CTICIDR1 can be accessed through the external debug interface, offset 0xFF4.

C11.15 CTI Component Identification Register 2

The CTICIDR2 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTICIDR2 by condition code is:

Off	DLK	OSLK	EPMAID	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTICIDR2 is in the Debug power domain.

CTICIDR2 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-10 CTICIDR2 bit assignments

[31:8]

Reserved, RES0.

PRMBL_2, [7:0]

0x05 Preamble byte 2.

CTICIDR2 can be accessed through the external debug interface, offset 0xFF8.

C11.16 CTI Component Identification Register 3

The CTICIDR3 characteristics are:

Purpose

Provides information to identify a CTI component.

Usage constraints

The accessibility of CTICIDR3 by condition code is:

Off	DLK	OSLK	EPMA	SLK	Default
-	-	-	-	RO	RO

C11.2 External register access permissions to the CTI registers on page C11-516 describes the condition codes.

Configurations

CTICIDR3 is in the Debug power domain.

CTICIDR3 is optional to implement in the external register interface.

Attributes

See the register summary in *C11.1 Cross trigger register summary on page C11-514*.



Figure C11-11 CTICIDR3 bit assignments

[31:8]

Reserved, RES0.

PRMBL_3, [7:0]

0xB1 Preamble byte 3.

CTICIDR3 can be accessed through the external debug interface, offset 0xFFC.

Part D
Appendices

Appendix A

Signal Descriptions

This appendix describes the signals at the external interfaces of the processor.

It contains the following sections:

- *A.1 About the signal descriptions on page Appx-A-534.*
- *A.2 Processor configuration signals on page Appx-A-535.*
- *A.3 Clock signals on page Appx-A-536.*
- *A.4 Reset signals on page Appx-A-537.*
- *A.5 GIC signals on page Appx-A-538.*
- *A.6 Generic Timer signals on page Appx-A-541.*
- *A.7 Power management signals on page Appx-A-542.*
- *A.8 L2 error signals on page Appx-A-544.*
- *A.9 ACP interface signals on page Appx-A-545.*
- *A.10 Broadcast signals for the memory interface on page Appx-A-547.*
- *A.11 AXI interface signals on page Appx-A-548.*
- *A.12 ACE interface signals on page Appx-A-550.*
- *A.13 CHI interface signals on page Appx-A-554.*
- *A.14 Debug signals on page Appx-A-557.*
- *A.15 APB interface signals on page Appx-A-559.*
- *A.16 ATB interface signals on page Appx-A-560.*
- *A.17 ETM signals on page Appx-A-561.*
- *A.18 PMU interface signals on page Appx-A-562.*
- *A.19 CTI interface signals on page Appx-A-563.*
- *A.20 DFT interface signals on page Appx-A-564.*
- *A.21 MBIST interface signals on page Appx-A-565.*

A.1 About the signal descriptions

The tables in this appendix provide direction information and high-level descriptions about the signals at the external interfaces of the processor.

Some of the buses include a configurable width field, <Signal>[CN:0], where CN = 0, 1, 2, or 3, to encode up to four cores. For example:

- **nIRQ[0]** represents a core 0 interrupt request.
- **nIRQ[2]** represents a core 2 interrupt request.

Some signals are specified in the form <signal>x where x = 0, 1, 2 or 3 to reference core 0, core 1, core 2, core 3. If a core is not present, the corresponding pin is removed. For example:

- **PMUEVENT0[29:0]** represents the core 0 PMU event bus.
- **PMUEVENT3[29:0]** represents the core 3 PMU event bus.

The number of signals changes depending on the configuration. For example, the CHI interface signals are not present when the processor is configured to have an ACE memory interface.

A.2 Processor configuration signals

The processor samples configuration signals only during cluster reset.

Table A-1 Processor configuration signals

Signal	Direction	Description
CFGEND[CN:0]	Input	Endianness configuration at reset. It sets the initial value of SCTLR_EL3.EE and SCTR_S.EE: 0 LOW. 1 HIGH.
CLUSTERIDAFF1[7:0]	Input	Value read in MPIDR.Aff1. This signal is sampled only during processor reset.
CLUSTERIDAFF2[7:0]	Input	Value read in MPIDR.Aff2. This signal is sampled only during processor reset.
CRYPTODISABLE[CN:0]	Input	Disabling the Cryptographic Extensions.
RVBARADDRx[39:2]	Input	Reset Vector Base Address for executing in 64-bit state.

Related information

[B1.71 System Control Register, EL1](#) on page B1-256.

[B1.65 Multiprocessor Affinity Register, EL1](#) on page B1-245.

A.3 Clock signals

The processor uses a single standard clock signal.

Table A-2 Clock signal

Signal	Direction	Description
CLKIN	Input	Global clock

Related information

[A3.1 Clocks on page A3-44.](#)

A.4 Reset signals

The processor uses a set of reset signals.

Table A-3 Reset and reset control signals

Signal	Direction	Description
nCPUPORESET[CN:0]	Input	Processor powerup reset: 0 Apply reset to all processor logic. 1 Do not apply reset to all processor logic. Processor logic includes Advanced SIMD and floating-point, debug, ETM trace unit, breakpoint and watchpoint logic.
nCORERESET[CN:0]	Input	Individual core resets excluding debug and ETM trace unit: 0 Apply reset to processor logic. 1 Do not apply reset to processor logic.
nPRESETDBG	Input	See A.15 APB interface signals on page Appx-A-559.
nL2RESET	Input	L2 memory system reset: 0 Apply reset to the shared L2 memory system controller. 1 Do not apply reset to the shared L2 memory system controller.
nMBISTRESET	Input	See A.21 MBIST interface signals on page Appx-A-565.
L2RSTDISABLE	Input	Disable the automatic invalidation of the L2 cache at reset: 0 Hardware resets the L2 cache. 1 Hardware does not reset the L2 cache. This signal is sampled only during processor reset.
WARMRSTREQ[CN:0]	Output	Request for a processor warm reset: 0 Do not apply warm reset. 1 Apply warm reset.
DBGRSTREQ[CN:0]	Output	Warm reset request.
DBGL1RSTDISABLE	Input	Disable the automatic invalidation of the L1 data cache at processor reset: 0 Enable automatic invalidation of L1 data cache on reset. 1 Disable automatic invalidation of L1 data cache on reset. This signal is sampled only during processor reset.

Related information

[A3.3 Resets](#) on page A3-46.

A.5 GIC signals

The processor uses a range of signals for global disable, base address definition, interrupt types, and Distributor messaging.

This interface exists only if the processor is configured to use the GIC CPU interface. However, the first seven signals in the following table are present even when the processor is configured without a GIC CPU interface.

Table A-4 GIC signals

Signal	Direction	Description
nFIQ[CN:0]	Input	<p>FIQ request. Active-LOW, level sensitive, asynchronous FIQ interrupt request:</p> <p>0 Activate FIQ interrupt. 1 Do not activate FIQ interrupt.</p> <p>The processor treats the nFIQ input as level-sensitive. The nFIQ input must be asserted until the processor acknowledges the interrupt.</p>
nIRQ[CN:0]	Input	<p>IRQ request input lines. Active-LOW, level sensitive, asynchronous interrupt request:</p> <p>0 Activate interrupt. 1 Do not activate interrupt.</p> <p>The processor treats the nIRQ input as level-sensitive. The nIRQ input must be asserted until the processor acknowledges the interrupt.</p>
nSEI[CN:0]	Input	<p>System Error Interrupt request. Active-LOW, edge sensitive:</p> <p>0 Activate SEI request. 1 Do not activate SEI request.</p> <p>The processor treats nSEI as edge-sensitive. The nSEI signal must be sent as a pulse to the processor.</p> <p>Asserting the nSEI input causes a SError interrupt. The ESR_ELx.ISS field is set.</p>
nVFIQ[CN:0]	Input	<p>Virtual FIQ request. Active-LOW, level sensitive, asynchronous FIQ interrupt request:</p> <p>0 Activate FIQ interrupt. 1 Do not activate FIQ interrupt.</p> <p>The processor treats the nVFIQ input as level-sensitive. The nVFIQ input must be asserted until the processor acknowledges the interrupt. If the GIC is enabled by tying GICCDISABLE LOW, nVFIQ must be tied off to HIGH. If the GIC is disabled by tying GICCDISABLE HIGH, nVFIQ can be driven by an external GIC in the SoC.</p>
nVIRQ[CN:0]	Input	<p>Virtual IRQ request. Active-LOW, level sensitive, asynchronous interrupt request:</p> <p>0 Activate interrupt. 1 Do not activate interrupt.</p> <p>The processor treats nVIRQ as level-sensitive. nVIRQ must be asserted until the processor acknowledges the interrupt. If the GIC is enabled by tying GICCDISABLE LOW, nVIRQ must be tied off to HIGH. If the GIC is disabled by tying GICCDISABLE HIGH, nVIRQ can be driven by an external GIC in the SoC.</p>

Table A-4 GIC signals (continued)

Signal	Direction	Description
nVSEI[CN:0]	Input	Virtual System Error Interrupt request. Active-LOW, edge sensitive: 0 Activate virtual SEI request. 1 Do not activate virtual SEI request. The processor treats nVSEI as edge-sensitive. The nVSEI signal must be sent as a pulse to the processor. Asserting nVSEI causes a SError interrupt. The ESR_EL1.ISS field is set.
nREI[CN:0]	Input	RAM Error Interrupt request. Active-LOW, edge sensitive: 0 Activate REI request. Reports an asynchronous RAM error in the system. 1 Do not activate REI request. The processor treats nREI as edge-sensitive. The nREI signal must be sent as a pulse to the processor. Asserting the nREI input causes a SError interrupt. The ESR_ELx.ISS field is set.
nVCPUMNTIRQ[CN:0]	Output	Virtual CPU interface maintenance interrupt PPI output.
PERIPBASE[39:18]	Input	Specifies the base address for the GIC registers. This value is sampled into CBAR at reset.
GICCDISABLE	Input	Globally disables the GIC CPU interface logic and routes the external signals directly to the processor: 0 Enable the GIC CPU interface logic. 1 Disable the GIC CPU interface logic and route the legacy nIRQ , nFIQ , nVIRQ , and nVFIQ signals directly to the processor. Drive this signal HIGH when you are using a legacy interrupt controller such as the GIC-400 which does not support GICv3 or GICv4.

Table A-5 AXI4 Stream Protocol signals for messages from the Distributor to the GIC CPU Interface

Signal	Direction	Description
ICDTVALID	Input	Indicates that the master is driving a valid transfer.
ICDTREADY	Output	Indicates that the slave can accept a transfer in the current cycle.
ICDTDATA[15:0]	Input	Primary payload for the data that is passing across the interface.
ICDTLAST	Input	Indicates the boundary of a packet.
ICDTDEST[1:0]	Input	Routing information for the data stream.

Table A-6 AXI4 Stream Protocol signals for messages from the GIC CPU Interface to the Distributor

Signal	Direction	Description
ICCTVALID	Output	Indicates that the master is driving a valid transfer.
ICCTREADY	Input	Indicates that the slave can accept a transfer in the current cycle.
ICCTDATA[15:0]	Output	Primary payload for the data that is passing across the interface.
ICCTLAST	Output	Indicates the boundary of a packet.
ICCTID[1:0]	Output	Data stream identifier.

Related information

B1.39 Exception Syndrome Register, EL1 on page B1-195.

B1.28 Configuration Base Address Register, EL1 on page B1-173.

A.6 Generic Timer signals

The processor uses a standard set of signals for the Generic Timer.

Table A-7 Generic Timer signals

Signal	Direction	Description
nCNTHPIRQ[CN:0]	Output	Hypervisor physical timer event.
nCNTPNSIRQ[CN:0]	Output	Non-secure physical timer event.
nCNTPSIRQ[CN:0]	Output	Secure physical timer event.
nCNTVIRQ[CN:0]	Output	Virtual physical timer event.
CNTCLKEN	Input	Counter clock enable. This clock enable must be asserted one cycle before the CNTVALUEB bus.
CNTVALUEB[63:0]	Input	Global system counter value in binary format.

Related information

[A2.4 About the Generic Timer on page A2-41.](#)

A.7 Power management signals

The processor has retention and non-retention signals for power management.

Table A-8 Non-Retention power management signals

Signal	Direction	Description
CLREXMONREQ	Input	Clearing of the external global exclusive monitor request. When this signal is asserted, it acts as a WFE wake-up event to all the cores in the processor device.
CLREXMONACK	Output	Clearing of the external global exclusive monitor acknowledge.
EVENTI	Input	Event input for processor wake-up from WFE state.
EVENTO	Output	Event output. Active when a SEV instruction is executed.
STANDBYWFI[CN:0]	Output	Indicates whether a core is in WFI low-power state: 0 Core not in WFI low-power state. 1 Core in WFI low-power state. This is the reset condition.
STANDBYWFE[CN:0]	Output	Indicates whether a core is in WFE low-power state: 0 Core not in WFE low-power state. 1 Core in WFE low-power state.
STANDBYWFIL2	Output	Indicates whether the L2 memory system is in WFI low-power state. This signal is active when the following conditions are met: <ul style="list-style-type: none"> • All cores are in WFI low-power state, held in reset, or nL2RESET is asserted LOW. • In an ACE configuration, ACINACTM is asserted HIGH. • In a CHI configuration, SINACT is asserted HIGH. • If ACP has been configured, AINACTS is asserted HIGH. • L2 memory system is idle.
L2FLUSHREQ	Input	L2 hardware flush request.
L2FLUSHDONE	Output	L2 hardware flush complete.
SMPEN[CN:0]	Output	Indicates whether a core is taking part in coherency.
DBGNOPWRDWN[CN:0]	Output	Request not to power down the core: 0 Do not request that the core stays powered-up. 1 Request that the core stays powered-up.
DBGPWRUPREQ[CN:0]	Output	Core power-up request: 0 Do not request that the core is powered up. 1 Request that the core is powered up.
DBGPWRDUP[CN:0]	Input	Core powered up 0 Core is powered down. 1 Core is powered up.

Table A-9 Retention power management signals

Signal	Direction	Description
CPUQACTIVE[CN:0]	Output	Indicates whether the referenced core is active
CPUQREQn[CN:0]	Input	Indicates that the power controller is ready to enter or exit retention for the referenced core
CPUQDENY[CN:0]	Output	Indicates that the referenced core denies the power controller retention request
CPUQACCEPTn[CN:0]	Output	Indicates that the referenced core accepts the power controller retention request
NEONQACTIVE[CN:0]	Output	Indicates whether the referenced Advanced SIMD and Floating-point block is active
NEONQREQn[CN:0]	Input	Indicates that the power controller is ready to enter or exit retention for the referenced Advanced SIMD and Floating-point block
NEONQDENY[CN:0]	Output	Indicates that the referenced Advanced SIMD and Floating-point block denies the power controller retention request
NEONQACCEPTn[CN:0]	Output	Indicates that the referenced Advanced SIMD and Floating-point block accepts the power controller retention request
L2QACTIVE	Output	Indicates whether the L2 data RAMs are active
L2QREQn	Input	Indicates that the power controller is ready to enter or exit retention for the L2 data RAMs
L2QDENY	Output	Indicates that the L2 data RAMs deny the power controller retention request
L2QACCEPTn	Output	Indicates that the L2 data RAMs accept the power controller retention request

Related information

Chapter A4 Power Management on page A4-49.

A.8 L2 error signals

The processor has signals for errors in the Level 2 cache.

Table A-10 L2 error signals

Signal	Direction	Description
nEXTERRIRQ	Output	Error indicator for memory transactions with a write response error condition.
nINTERRIRQ	Output	Error indicator for L2 RAM double-bit ECC error.

Related information

[A7.5 Handling of external aborts on page A7-93.](#)

A.9 ACP interface signals

The AXI protocol supports clock, configuration, and data handling signals if the processor implements the ACP slave interface to an external master to make coherent request to the shared L2 cache of the cluster.

This interface exists only if the processor is configured to have the ACP interface.

All ACP channels must be balanced with respect to **CLKIN** and timed relative to **ACLKENS**.

Table A-11 ACP clock and Configuration signals

Signal	Direction	Description
ACLKENS	Input	AXI slave bus clock enable.
AINACTS	Input	<p>ACP master is inactive and is not participating in coherency. There must be no outstanding transactions when the master asserts this signal, and while it is asserted the master must not send any new transactions:</p> <p>0 ACP Master is active.</p> <p>1 ACP Master is inactive.</p> <p>This signal must be asserted before the processor enters the low-power L2 WFI state.</p>

Table A-12 ACP write address channel signals

Signal	Direction	Description
AWREADY	Output	Write address ready
AWVALID	Input	Write address valid
AWIDS[4:0]	Input	Write address ID
AWADDRS[39:0]	Input	Write address
AWLENS[7:0]	Input	Write burst length
AWCACHES[3:0]	Input	Write cache type
AWUSERS[1:0]	Input	<p>Write attributes:</p> <p>[0] Inner Shareable.</p> <p>[1] Outer Shareable.</p>
AWPROTS[2:0]	Input	Write protection type

Table A-13 ACP write data channel signals

Signal	Direction	Description
WREADY	Output	Write data ready
WVALID	Input	Write data valid
WDATAS[127:0]	Input	Write data
WSTRBS[15:0]	Input	Write byte-lane strobes
WLASTS	Input	Write data last transfer indication

Table A-14 ACP write response channel signals

Signal	Direction	Description
BREADYS	Input	Write response ready
BVALIDS	Output	Write response valid
BIDS[4:0]	Output	Write response ID
BRESPS[1:0]	Output	Write response

Table A-15 ACP read address channel signals

Signal	Direction	Description
ARREADYS	Output	Read address ready
ARVALIDS	Input	Read address valid
ARIDS[4:0]	Input	Read address ID
ARADDRS[39:0]	Input	Read address
ARLENS[7:0]	Input	Read burst length
ARCACHES[3:0]	Input	Read cache type
ARUSERS[1:0]	Input	Read attributes: [0] Inner Shareable. [1] Outer Shareable.
ARPROTS[2:0]	Input	Read protection type

Table A-16 ACP read data channel signals

Signal	Direction	Description
RREADYS	Input	Read data ready
RVALIDS	Output	Read data valid
RIDS[4:0]	Output	Read data ID
RDATAS[127:0]	Output	Read data
RRESPS[1:0]	Output	Read response
RLASTS	Output	Read data last transfer indication

A.10 Broadcast signals for the memory interface

The processor has broadcast signals for the memory interface. These signals are only sampled at processor reset.

The signals in the following table only exist if the processor is configured to have an ACE or CHI memory interface.

Table A-17 Broadcast signals

Signal	Direction	Description
BROADCASTCACHEMAINT	Input	Enable broadcasting of cache maintenance operations to downstream caches: 0 Cache maintenance operations are not broadcast to downstream caches. 1 Cache maintenance operations are broadcast to downstream caches.
BROADCASTINNER	Input	Enable broadcasting of Inner Shareable transactions: 0 Inner Shareable transactions are not broadcast externally. 1 Inner Shareable transactions are broadcast externally. If BROADCASTINNER is tied HIGH, you must also tie BROADCASTOUTER HIGH.
BROADCASTOUTER	Input	Enable broadcasting of outer shareable transactions: 0 Outer Shareable transactions are not broadcast externally. 1 Outer Shareable transactions are broadcast externally.

A.11 AXI interface signals

The AXI protocol supports clock, configuration, and data handling signals when the processor uses this protocol for the master memory interface.

This interface exists only if the processor is configured to have the AXI interface.

All AXI channels must be balanced with respect to **CLKIN** and timed relative to **ACLKENM**.

Table A-18 AXI clock and configuration signals

Signal	Direction	Description
ACLKENM	Input	AXI Master bus clock enable. See A3.1 Clocks on page A3-44 for more information.
RDMEMATTR[7:0]	Output	Read request memory attributes.
WRMEMATTR[7:0]	Output	Write request memory attributes.

Table A-19 AXI write address channel signals

Signal	Direction	Description
AWADDRM[39:0]	Output	Write address.
AWBURSTM[1:0]	Output	Write burst type.
AWCACHM[3:0]	Output	Write cache type.
AWIDM[4:0]	Output	Write address ID.
AWLENM[7:0]	Output	Write burst length.
AWLOCKM	Output	Write lock type.
AWPROTM[2:0]	Output	Write protection type.
AWREADYM	Input	Write address ready.
AWSIZEM[2:0]	Output	Write burst size.
AWVALIDM	Output	Write address valid.

Table A-20 AXI write data channel signals

Signal	Direction	Description
WDATAM[127:0]	Output	Write data
WIDM[4:0]	Output	Write data ID
WLASTM	Output	Write data last transfer indication
WREADYM	Input	Write data ready
WSTRBM[15:0]	Output	Write byte-lane strobes
WVALIDM	Output	Write data valid

Table A-21 AXI write data response channel signals

Signal	Direction	Description
BIDM[4:0]	Input	Write response ID
BREADYM	Output	Write response ready

Table A-21 AXI write data response channel signals (continued)

Signal	Direction	Description
BRESPM[1:0]	Input	Write response
BVALIDM	Input	Write response valid

Table A-22 AXI read address channel signals

Signal	Direction	Description
ARADDRM[39:0]	Output	Read address.
ARBURSTM[1:0]	Output	Read burst type.
ARCACHEM[3:0]	Output	Read cache type
ARIDM[5:0]	Output	Read address ID
ARLENM[7:0]	Output	Read burst length
ARLOCKM	Output	Read lock type
ARPROTM[2:0]	Output	Read protection type
ARREADYM	Input	Read address ready
ARSIEM[2:0]	Output	Read burst size
ARVALIDM	Output	Read address valid

Table A-23 AXI read data channel signals

Signal	Direction	Description
RDATAM[127:0]	Input	Read data
RIDM[5:0]	Input	Read data ID
RLASTM	Input	Read data last transfer indication
RREADYM	Output	Read data ready
RRESPM[1:0]	Input	Read data response
RVALIDM	Input	Read data valid

Related information

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, and ACE and ACE-Lite.

A.12 ACE interface signals

The ACE protocol supports clock, configuration, and data handling signals when the processor uses this protocol for the master memory interface.

This interface exists only if the Cortex-A34 processor is configured to have the ACE interface.

All ACE channels must be balanced with respect to **CLKIN** and timed relative to **ACLKENM**.

Table A-24 ACE clock and configuration signals

Signal	Direction	Description
ACLKENM	Input	ACE Master bus clock enable.
ACINACTM	Input	Snoop interface is inactive and not participating in coherency: 0 Snoop interface is active. 1 Snoop interface is inactive.
RDMEMATTR[7:0]	Output	Read request memory attributes.
WRMEMATTR[7:0]	Output	Write request memory attributes.

Table A-25 ACE write address channel signals

Signal	Direction	Description
AWADDRM[43:0]	Output	Write address.
AWBARM[1:0]	Output	Write barrier type.
AWBURSTM[1:0]	Output	Write burst type.
AWCACHEM[3:0]	Output	Write cache type.
AWDOMAINM[1:0]	Output	Write shareability domain type.
AWIDM[4:0]	Output	Write address ID.
AWLENM[7:0]	Output	Write burst length.
AWLOCKM	Output	Write lock type.
AWPROTM[2:0]	Output	Write protection type.
AWREADYM	Input	Write address ready.
AWSIZEM[2:0]	Output	Write burst size.
AWSNOOPM[2:0]	Output	Write snoop request type.
AWUNIQUEM	Output	For WriteBack, WriteClean and WriteEvict transactions. Indicates that the write is: 0 Shared. 1 Unique.
AWVALIDM	Output	Write address valid.

Table A-26 ACE write data channel signals

Signal	Direction	Description
WDATAM[127:0]	Output	Write data
WIDM[4:0]	Output	Write data ID
WLASTM	Output	Write data last transfer indication
WREADYM	Input	Write data ready
WSTRBM[15:0]	Output	Write byte-lane strobes
WVALIDM	Output	Write data valid

Table A-27 ACE write data response channel signals

Signal	Direction	Description
BIDM[4:0]	Input	Write response ID
BREADYM	Output	Write response ready
BRESPM[1:0]	Input	Write response
BVALIDM	Input	Write response valid

Table A-28 ACE read address channel signals

Signal	Direction	Description
ARADDRM[43:0]	Output	Read address. The top 4 bits communicate only the ACE virtual address for DVM messages. The top 4 bits are Read-as-Zero if a DVM message is not being broadcast.
ARBARM[1:0]	Output	Read barrier type.
ARBURSTM[1:0]	Output	Read burst type.
ARCACHEM[3:0]	Output	Read cache type.
ARDOMAINM[1:0]	Output	Read shareability domain type.
ARIDM[5:0]	Output	Read address ID.
ARLENM[7:0]	Output	Read burst length.
ARLOCKM	Output	Read lock type.
ARPROTM[2:0]	Output	Read protection type.
ARREADYM	Input	Read address ready.
ARSIZEM[2:0]	Output	Read burst size.
ARSNOOPM[3:0]	Output	Read snoop request type.
ARVALIDM	Output	Read address valid.

Table A-29 ACE read data channel signals

Signal	Direction	Description
RDATAM[127:0]	Input	Read data
RIDM[5:0]	Input	Read data ID
RLASTM	Input	Read data last transfer indication
RREADYM	Output	Read data ready
RRESPM[3:0]	Input	Read data response
RVALIDM	Input	Read data valid

Table A-30 ACE coherency address channel signals

Signal	Direction	Description
ACADDRM[43:0]	Input	Snoop address. The top 4 bits communicate only the ACE virtual address for DVM messages.
ACPROTM[2:0]	Input	Snoop protection type.
ACREADYM	Output	Master ready to accept snoop address.
ACSNOOPM[3:0]	Input	Snoop request type.
ACVALIDM	Input	Snoop address valid.

Table A-31 ACE coherency response channel signals

Signal	Direction	Description
CRREADYM	Input	Slave ready to accept snoop response
CRVALIDM	Output	Snoop response
CRRESPM[4:0]	Output	Snoop response valid

Table A-32 ACE coherency data channel handshake signals

Signal	Direction	Description
CDDATAM[127:0]	Output	Snoop data
CDLASTM	Output	Snoop data last transform
CDREADYM	Input	Slave ready to accept snoop data
CDVALIDM	Output	Snoop data valid

Table A-33 ACE read and write acknowledge signals

Signal	Direction	Description
RACKM	Output	Read acknowledge
WACKM	Output	Write acknowledge

Related information

A3.1 Clocks on page A3-44.

ARM® AMBA® AXI and ACE Protocol Specification AXI3, AXI4, and AXI4-Lite, and ACE and ACE-Lite.

A.13 CHI interface signals

The CHI protocol supports clock, configuration, data handling, and address map signals when the processor uses this protocol for the master memory interface.

This interface exists only if the processor is configured to have the CHI interface.

Table A-34 CHI clock and configuration signals

Signal	Direction	Description
SCLKEN	Input	CHI interface bus clock enable
SINACT	Input	CHI snoop active
NODEID[6:0]	Input	Cortex-A34 CHI Node Identifier
RXSACTIVE	Input	Receive pending activity indicator
TXSACTIVE	Output	Transmit pending activity indicator
RXLINKACTIVEREQ	Input	Receive link active request
RXLINKACTIVEACK	Output	Receive link active acknowledge
TXLINKACTIVEREQ	Output	Transmit link active request
TXLINKACTIVEACK	Input	Transmit link active acknowledge
REQMEMATTR[7:0]	Output	Request memory attributes

Table A-35 CHI transmit request virtual channel signals

Signal	Direction	Description
TXREQFLITPEND	Output	Transmit request flit pending
TXREQFLITV	Output	Transmit request flit valid
TXREQFLIT[99:0]	Output	Transmit request flit payload
TXREQLCRDV	Input	Transmit request link-layer credit valid

Table A-36 CHI transmit response virtual channel signals

Signal	Direction	Description
TXRSPFLITPEND	Output	Transmit response flit pending
TXRSPFLITV	Output	Transmit response flit valid
TXRSPFLIT[44:0]	Output	Transmit response flit
TXRSPLCRDV	Input	Transmit response link-layer credit valid

Table A-37 CHI transmit data virtual channel signals

Signal	Direction	Description
TXDATFLITPEND	Output	Transmit data flit pending
TXDATFLITV	Output	Transmit data flit valid
TXDATFLIT[193:0]	Output	Transmit data flit
TXDATLCRDV	Input	Transmit data link-layer credit valid

Table A-38 CHI receive snoop virtual channel signals

Signal	Direction	Description
RXSNPFLITPEND	Input	Receive snoop flit pending
RXSNPFLITV	Input	Receive snoop flit valid
RXSNPFLIT[64:0]	Input	Receive snoop flit
RXSNPLCRDV	Output	Receive snoop link-layer credit valid

Table A-39 CHI receive response virtual channel signals

Signal	Direction	Description
RXRSPFLITPEND	Input	Receive response flit pending
RXRSPFLITV	Input	Receive response flit valid
RXRSPFLIT[44:0]	Input	Receive response flit
RXRSPLCRDV	Output	Receive response link-layer credit valid

Table A-40 CHI receive Data virtual channel signals

Signal	Direction	Description
RXDATFLITPEND	Input	Receive data flit pending
RXDATFLITV	Input	Receive data flit valid
RXDATFLIT[193:0]	Input	Receive data flit
RXDATLCRDV	Output	Receive data link-layer credit valid

Table A-41 CHI system address map signals

Signal	Direction	Description
SAMADDRMAP0[1:0]	Input	Region mapping, 0 – 512MB
SAMADDRMAP1[1:0]	Input	Region mapping, 512MB – 1GB
SAMADDRMAP2[1:0]	Input	Region mapping, 1GB – 1.5GB
SAMADDRMAP3[1:0]	Input	Region mapping, 1.5GB – 2GB
SAMADDRMAP4[1:0]	Input	Region mapping, 2GB – 2.5GB
SAMADDRMAP5[1:0]	Input	Region mapping, 2.5GB – 3GB
SAMADDRMAP6[1:0]	Input	Region mapping, 3GB – 3.5GB
SAMADDRMAP7[1:0]	Input	Region mapping, 3.5GB – 4GB
SAMADDRMAP8[1:0]	Input	Region mapping, 4GB – 8GB
SAMADDRMAP9[1:0]	Input	Region mapping, 8GB – 16GB
SAMADDRMAP10[1:0]	Input	Region mapping, 16GB – 32GB
SAMADDRMAP11[1:0]	Input	Region mapping, 32GB – 64GB
SAMADDRMAP12[1:0]	Input	Region mapping, 64GB – 128GB
SAMADDRMAP13[1:0]	Input	Region mapping, 128GB – 256GB

Table A-41 CHI system address map signals (continued)

Signal	Direction	Description
SAMADDRMAP14[1:0]	Input	Region mapping, 256GB – 512GB
SAMADDRMAP15[1:0]	Input	Region mapping, 512GB – 1TB
SAMMNBASE[39:24]	Input	MN base address SAMMNBASE must reside in a SAMADDRMAP_x[1:0] that corresponds to the HN-I.
SAMMNNODEID[6:0]	Input	MN node ID
SAMHNI0NODEID[6:0]	Input	HN-I 0 node ID
SAMHNI1NODEID[6:0]	Input	HN-I 1 node ID
SAMHNF0NODEID[6:0]	Input	HN-F 0 node ID
SAMHNF1NODEID[6:0]	Input	HN-F 1 node ID
SAMHNF2NODEID[6:0]	Input	HN-F 2 node ID
SAMHNF3NODEID[6:0]	Input	HN-F 3 node ID
SAMHNF4NODEID[6:0]	Input	HN-F 4 node ID
SAMHNF5NODEID[6:0]	Input	HN-F 5 node ID
SAMHNF6NODEID[6:0]	Input	HN-F 6 node ID
SAMHNF7NODEID[6:0]	Input	HN-F 7 node ID
SAMHNFMODE[2:0]	Input	HN-F interleaving module

A.14 Debug signals

The processor has the following debug signals.

Table A-42 Debug signals

Signal	Direction	Description
DBGROMADDR[39:12]	Input	Debug ROM base address. Specifies bits[39:12] of the ROM table physical address. If the address cannot be determined, tie this signal LOW. This signal is sampled only during processor reset.
DBGROMADDRV	Input	Debug ROM base address valid. If the debug ROM address cannot be determined, tie this signal LOW. This signal is sampled only during processor reset.
DBGACK[CN:0]	Output	Debug acknowledge: 0 External debug request not acknowledged. 1 External debug request acknowledged.
nCOMMIRQ[CN:0]	Output	Communications channel receive or transmit interrupt request 0 Request interrupt. 1 No interrupt request.
COMMRX[CN:0]	Output	Communications channel receive. Receive portion of Data Transfer Register full flag: 0 Empty. 1 Full.
COMMTX[CN:0]	Output	Communication transmit channel. Transmit portion of Data Transfer Register empty flag: 0 Full. 1 Empty.
EDBGRQ[CN:0]	Input	External debug request: 0 No external debug request. 1 External debug request. The processor treats the EDBGRQ input as level-sensitive. The EDBGRQ input must be asserted until the processor asserts DBGACK .
DBGEN[CN:0]	Input	Invasive debug enable: 0 Not enabled. 1 Enabled.
NIDEN[CN:0]	Input	Non-invasive debug enable: 0 Not enabled. 1 Enabled.

Table A-42 Debug signals (continued)

Signal	Direction	Description
SPIDEN[CN:0]	Input	Secure privileged invasive debug enable: 0 Not enabled. 1 Enabled.
SPNIDEN[CN:0]	Input	Secure privileged non-invasive debug enable: 0 Not enabled. 1 Enabled.
DBGRSTREQ[CN:0]	Output	Warm reset request.
DBGNOPWRDWN[CN:0]	Output	Request not to power down the core: 0 Do not request that the core stays powered up. 1 Request that the core stays powered up.
DBGPWRUPREQ[CN:0]	Output	Core power- up request: 0 Do not request that the core is powered up. 1 Request that the core is powered up.
DBGPWRDUP[CN:0]	Input	Core powered up: 0 Core is powered down. 1 Core is powered up.
DBGL1RSTDISABLE	Input	Disable the automatic invalidation of the L1 data cache at processor reset: 0 Enable automatic invalidation of L1 data cache on reset. 1 Disable automatic invalidation of L1 data cache on reset. This signal is sampled only during processor reset.

Related information

Chapter C1 Debug on page C1-295.

AArch64 debug registers.

Memory-mapped debug registers.

Chapter C7 Debug memory mapped registers on page C7-349.

Chapter C8 ROM table on page C8-375.

A.15 APB interface signals

The debug APB bus supports clock, reset, addressing, and data handling signals when the processor includes an APB interface to provide access to the debug and performance monitoring registers.

You must balance all APB interface signals with respect to **CLKIN** and time them relative to **PCLKENDBG**.

Table A-43 APB interface signals

Signal	Direction	Description
nPRESETDBG	Input	APB reset, active-LOW: 0 Apply reset to APB interface. 1 Do not apply reset to APB interface.
PADDRDBG[21:2]	Input	APB address bus.
PADDRDBG31	Input	APB address bus bit[31]: 0 Not an external debugger access. 1 External debugger access.
PCLKENDBG	Input	APB clock enable.
PENABLEDBG	Input	Indicates the second and subsequent cycles of an APB transfer.
PRDATADBG[31:0]	Output	APB read data.
PREADYDBG	Output	APB slave ready. An APB slave can deassert PREADYDBG to extend a transfer by inserting wait states.
PSELDBG	Input	Debug bus access.
PSLVERRDBG	Output	APB slave transfer error: 0 No transfer error. 1 Transfer error.
PWDATADBG[31:0]	Input	APB write data.
PWRITEDBG	Input	APB read or write signal: 0 Reads from APB. 1 Writes to APB.

A.16 ATB interface signals

The ATB bus supports clock and data handling signals when the processor includes an ATB interface for each core to output trace information for debugging.

This interface exists only if the processor is configured to have one or more ETMs.

You must balance all ATB interface signals with respect to **CLKIN** and time them relative to **ATCLKEN**.

Table A-44 ATB interface signals

Signal	Direction	Description
ATCLKEN	Input	ATB clock enable
ATREADYM_x	Input	ATB device ready
AFVALIDM_x	Input	FIFO flush request
ATDATAM_x[31:0]	Output	Data
ATVALIDM_x	Output	Data valid
ATBYTESM_x[1:0]	Output	Data size
AFREADYM_x	Output	FIFO flush finished
ATIDM_x[6:0]	Output	Trace source ID
SYNCREQM_x	Input	Synchronization request from the trace sink

A.17 ETM signals

The processor has signals to receive information from an external trace device.

This interface exists only if the processor is configured to have one or more ETMs.

Table A-45 ETM signals

Signal	Direction	Description
TSVALUEB[63:0]	Input	Timestamp in binary encoding

A.18 PMU interface signals

The processor uses the PMU signals to communicate with the external performance monitoring device.

Table A-46 PMU interface signals

Signal	Direction	Description
PMUEVENTx[29:0]	Output	PMU event bus
nPMUIRQ[CN:0]	Output	PMU interrupt request

A.19 CTI interface signals

The processor supports various cross-trigger signals when it implements the CTI.

Table A-47 CTI interface signals

Signal	Direction	Description
CTICHIN[3:0]	Input	Channel In
CTICHOUTACK[3:0]	Input	Channel Out acknowledge
CTICHOUT[3:0]	Output	Channel Out
CTICHINACK[3:0]	Output	Channel In acknowledge
CISBYPASS	Input	Channel interface sync bypass
CIHSBYPASS[3:0]	Input	Channel interface H/S bypass
CTHIRQ[CN:0]	Output	CTI interrupt, active-HIGH
CTHIRQACK[CN:0]	Input	CTI interrupt acknowledge

A.20 DFT interface signals

The processor uses the DFT signals to communicate with the external test device.

Table A-48 DFT interface signals

Signal	Direction	Description
DFTRAMHOLD	Input	Disable the RAM chip select during scan testing
DFTRSTDISABLE	Input	Disable internal synchronized reset during scan shift
DFTCGEN	Input	Clock gate enable, forces on the clock grids during scan shift
DFTMCPHOLD	Input	Disable Multicycle Paths on RAM interfaces

A.21 MBIST interface signals

The processor does not include an external MBIST address and data interface port. The MBIST address and data interface ports are internally tied-off in the design, and you can insert MBIST into the design before synthesis. The process of adding MBIST into the design can be done automatically by an EDA MBIST tool.

Table A-49 MBIST interface signals

Signal	Direction	Description
MBISTREQ	Input	MBIST test request
nMBISTRESET	Input	MBIST reset

Appendix B

Revisions

This appendix describes the technical changes between released issues of this book.

It contains the following sections:

- [B.1 Revisions on page Appx-B-568](#).

B.1 Revisions

This section describes the technical changes between released issues of this document.

Table B-1 Issue 0000-00

Change	Location	Affects
First release for r0p0.	-	-

Table B-2 Issue 0001-00

Change	Location	Affects
First release for r0p1.	On front page and in document history table. <i>B1.64 Main ID Register, EL1</i> on page B1-243. <i>B2.3 CPU Interface Identification Register</i> on page B2-284. <i>B2.8 VM CPU Interface Identification Register</i> on page B2-289. <i>C7.10 External Debug Peripheral Identification Register 1</i> on page C7-364. <i>C8.8 ROM Table Peripheral Identification Register 2</i> on page C8-385. <i>C9.10 Performance Monitors Peripheral Identification Register 2</i> on page C9-412. <i>C10.13 Trace ID Register</i> on page C10-440. <i>C10.68 ETM Peripheral Identification Register 2</i> on page C10-503. <i>C11.8 CTI Peripheral Identification Register 2</i> on page C11-522.	r0p1
Bits [9:0] updated in CPTR_EL3.	<i>B1.33 Architectural Feature Trap Register, EL3</i> on page B1-182.	All versions
References to internal memory-mapped removed.	<i>B1.65 Multiprocessor Affinity Register, EL1</i> on page B1-245. <i>C6.1 AArch64 debug register summary</i> on page C6-340. <i>C7.1 Memory-mapped debug register summary</i> on page C7-350. <i>C9.5 Memory-mapped PMU register summary</i> on page C9-405. <i>C11.1 Cross trigger register summary</i> on page C11-514.	All versions
nSEI, nREI, and nVSEI clarified in GIC signals table.	<i>A.5 GIC signals</i> on page Appx-A-538.	All versions