Arm® Neoverse™ CMN-650 Coherent Mesh Network

Software Developer Errata Notice

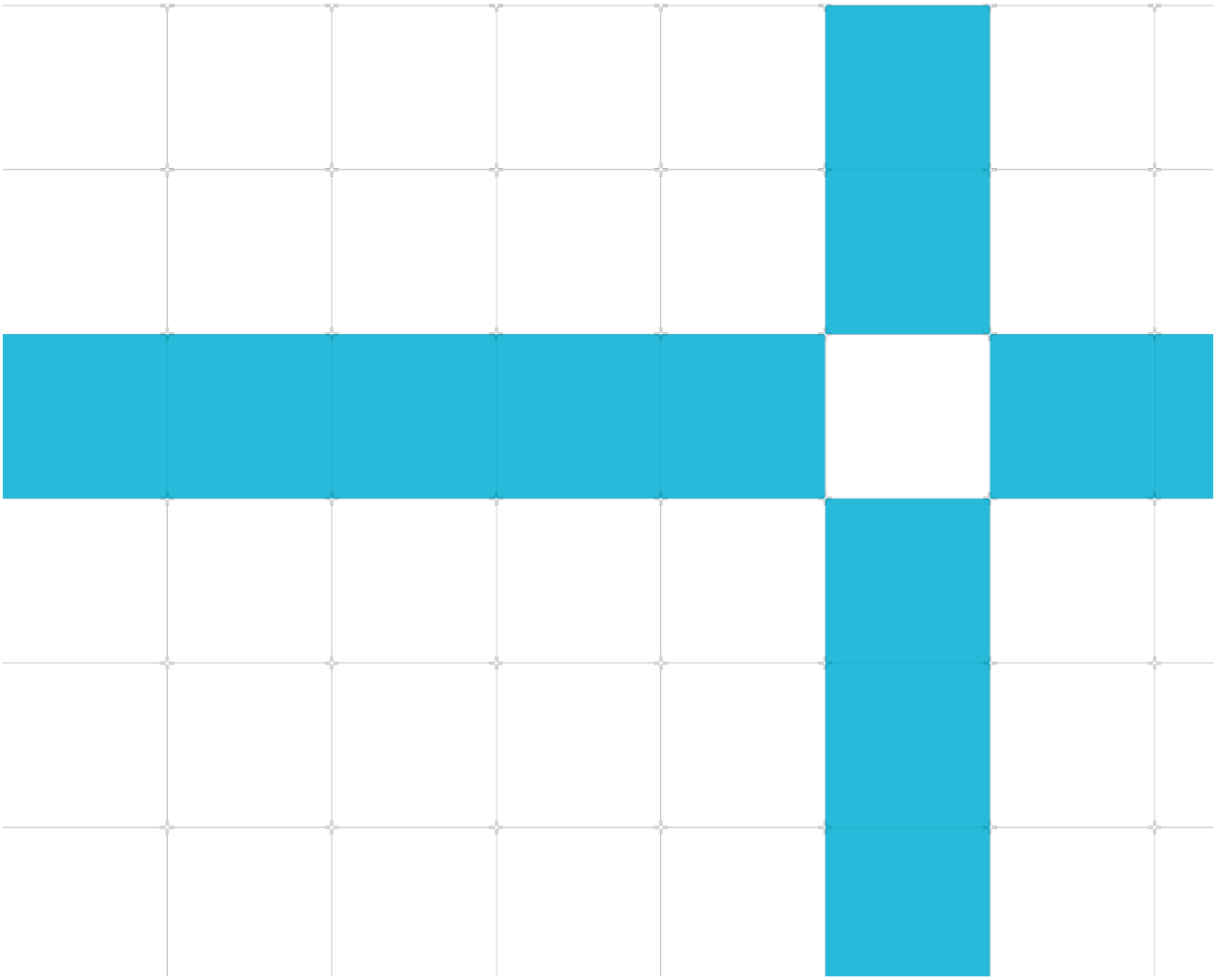
Date of issue: December 15, 2023

Non-Confidential

Document version: 11.0

Document ID: SDEN-1504336

This document contains all known errata since the r0p0 release of the product.



Non-confidential proprietary notice

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.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on Arm® Neoverse™ CMN-650 Coherent Mesh Network , create a ticket on **https://support.developer.arm.com**.

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

Inclusive language commitment

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

If you find offensive language in this document, please email **terms@arm.com**.

Contents

Introduction

Scope

This document describes errata categorized by level of severity. Each description includes:

- The current status of the erratum.
- Where the implementation deviates from the specification and the conditions required for erroneous behavior to occur.
- The implications of the erratum with respect to typical applications.
- The application and limitations of a workaround where possible.

Categorization of errata

Errata are split into three levels of severity and further qualified as common or rare:

Category A	A critical error. No workaround is available or workarounds are impactful. The error is likely to be common for many systems and applications.
Category A (Rare)	A critical error. No workaround is available or workarounds are impactful. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category B	A significant error or a critical error with an acceptable workaround. The error is likely to be common for many systems and applications.
Category B (Rare)	A significant error or a critical error with an acceptable workaround. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category C	A minor error.

Change Control

Errata are listed in this section if they are new to the document, or marked as "updated" if there has been any change to the erratum text. Fixed errata are not shown as updated unless the erratum text has changed. The **errata summary table** identifies errata that have been fixed in each product revision.

December 15, 2023: Changes in document version v11.0

ID	Status	Area	Category	Summary
3114475	New	Programmer	Category C	Transactions targeting the HN-D AXI interface might be stalled by a continuous stream of CMN configuration transactions

October 12, 2023: Changes in document version v10.0

No new or updated errata in this document version.

August 23, 2023: Changes in document version v9.0

ID	Status	Area	Category	Summary
3013640	New	Programmer	Category B	Write Stash can cause multi-copy atomicity issue
3031692	New	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

September 28, 2022: Changes in document version v8.0

ID	Status	Area	Category	Summary
2741287	New	Programmer	Category C	RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information

September 17, 2021: Changes in document version v7.0

No new or updated errata in this document version.

December 08, 2020: Changes in document version v6.0

No new or updated errata in this document version.

August 28, 2020: Changes in document version v5.0

ID	Status	Area	Category	Summary
1873199	New	Programmer	Category B	SECC error on ABF operation can cause coherency failures for other memory addresses

May 26, 2020: Changes in document version v4.0

No new or updated errata in this document version.

April 16, 2020: Changes in document version v3.0

ID	Status	Area	Category	Summary
1711597	New	Programmer	Category C	CMN-Rhodes Cbusy thresholds greater than 256 not functional

November 11, 2019: Changes in document version v2.0

No new or updated errata in this document version.

June 04, 2019: Changes in document version v1.0

No errata in this document version.

Errata summary table

The errata associated with this product affect the product versions described in the following table.

ID	Area	Category	Summary	Found in versions	Fixed in version
1873199	Programmer	Category B	SECC error on ABF operation can cause coherency failures for other memory addresses	r0p0, r1p0, r1p1, r1p2	r2p0
3013640	Programmer	Category B	Write Stash can cause multi-copy atomicity issue	r0p0, r1p0, r1p1, r1p2, r2p0	Open
1711597	Programmer	Category C	CMN-Rhodes Cbusy thresholds greater than 256 not functional	r1p0	r1p1
2741287	Programmer	Category C	RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information	r0p0, r1p0, r1p1, r1p2, r2p0	Open
3031692	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock	r0p0, r1p0, r1p1, r1p2, r2p0	Open
3114475	Programmer	Category C	Transactions targeting the HN-D AXI interface might be stalled by a continuous stream of CMN configuration transactions	r0p0, r1p0, r1p1, r1p2, r2p0	Open

Errata descriptions

Category A

There are no errata in this category.

Category A (rare)

There are no errata in this category.

Category B

1873199
SECC error on ABF operation can cause coherency failures for other memory addresses

Status

Affects: CMN-Rhodes
Fault Type: Programmer CAT-B
Fault Status: Present in r0p0, r1p0, r1p1, and r1p2. Fixed in r2p0.

Description

CMN-Rhodes supports Address Based Flush (ABF) where upper and lower system addresses can be programmed and then request hardware based engine to flush out that address range from all System Level Caches (SLC). This ABF state machine works in presence of other memory requests.

Single-bit ECC errors on the ABF accesses can corrupt the CMN Snoop Filter state, and result in coherency failures for other unrelated memory addresses.

Configurations Affected

Any configuration of CMN-Rhodes where ABF is used.

Conditions

This bug appears when following three conditions occur:

- SLC address from flush set/way is outside ABF programmed range AND
- SLC Tag read has single bit ECC error AND
- There is independent request in pipeline N cycles ahead of ABF request (where N is SLC_TAG_RAM_LATENCY)
  In this case, ABF request corrupts SF vector for independent request that's ahead of ABF causing coherency failure.

Implications

The ABF flush sequence can cause coherency fails for unrelated memory addresses during the sequence.

Workaround

Use the CMN power management features to flush the SLC, flushes the full SLC contents vs. the upper/lower range.

3013640
Write Stash can cause multi-copy atomicity issue

Status

Affects: CMN-650
Fault Type: Programmer Cat-B
Fault Status: r0p0, r1p0, r1p1, r1p2, r2p0. Open.

Description

CHI and AXI Write Stash operations can incorrectly get early completion before snooping is complete causing multi-copy atomicity issues.

For example, an RN-I or RN-D PCI MSI write issued after a Write Stash can result in the CPU having the older or stale copy of the Write Stash data at the time of the MSI interrupt.

Another example is an RN-I or RN-D write flag issued after completion of the Write Stash, the CPU can observe the flag update before the Write Stash data is updated.

Note that Arm CPUs do not issue Write Stash transactions.

Configurations affected

Any CMN configuration.

Conditions

This erratum occurs when the following conditions are met:

- RN-I or RN-D issues AXI Write Stash transaction with a valid StashNID targeting a CPU cache
- RN-I or RN-D issues another AXI transaction after receiving the completion for the Write Stash. For example, PCIE MSI write or write to flag address
- The Stash CPU can observe the results of the second transaction above before the Write Stash data is updated for the first

Implications

If the conditions are met, Write Stash could receive early completion while the Stash CPU still has old copy causing multi-copy atomicity issues.

Workarounds

The workaround is to send the result in Stash to the SLC instead of the CPU cache, by disabling stash snooping using por_hnf_aux_ctl.hnf_stash_disable

Category B (rare)

There are no errata in this category.

Category C

1711597
CMN-Rhodes Cbusy thresholds greater than 256 not functional

Status

Affects: CMN-Rhodes
Fault Type: Programmer CAT-C
Fault Status: Present in r1p0. Fixed in r1p1.

Description

HN-F has counters which track CBusy values from an SN over a number of transactions (programmable value). These counters are then used to estimate the SN's busyness level and throttle the outstanding transactions. These counters were sized incorrectly to 8-bits and hence overflow under certain conditions. Per the TRM, 128 or 256 are the allowed values for the transaction count.
This feature is not enabled by default in CMN-Rhodes. Its a user programmable feature to enable throttling of requests to SN.

Configurations Affected

All configurations of CMN-Rhodes R1P0 EAC

Conditions

For this bug to occur, below conditions must be met:

- *por_hnf_cfg_ctl* register's *hnf_adv_cbusy_mode_en* must be set to 1. This enables the advanced CBusy mode.
- *por_hnf_cbusy_sn_ctl* register's *hnf_cbusy_txn_cnt* field must be set to 256 AND
- All the responses from SN must have the same CBusy value of 11 or 10 or 01, over the 256 transaction responses

Implications

When the counter overflows, the absolute SN CBusy is calculated incorrectly. For example, if the SN responded with cBusy=11 (**very busy**) over the 256 transaction, the counter will instead roll over to 0 upon the 256th response. Hence the HNF will estimate the final CBusy value for this SN as CBusy=00 (**not busy**) and continue to send requests at full capacity. This may lead to lower performance as the SN will likely retry all requests. Instead, if the requests were throttled at the HN-F, the retry rate would be reduced and lead to overall higher performance.

Workaround

Instead of 256, if the user programs 255 in the transaction count, the feature is fully functional.

2741287
RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information

Status

Affects: CMN-650
Fault Type: Programmer CAT-C
Fault Status: r0p0, r1p0, r1p1, r1p2, r2p0. Open.

Description

The CMN Error Group Status Registers (ERRGSR) capture device instance error information for RAS events. The registers indicate the device instance within a device group. The registers are not updated correctly for the HN-I and SBSX device groups, so cannot be used to determine the device instances for RAS events.

Configurations Affected

All CMN-650 configurations that use RAS error logging.

Conditions

A RAS event triggered by an HN-I or SBSX device.

Implications

Software cannot use the HN-I or SBSX ERRGSR registers.

Workaround

The RAS handler must read the individual HN-I and SBSX instance RAS logging registers when RAS interrupts occur.

3031692
Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

Status

Affects: CMN-650
Fault Type: Programmer CAT-C
Fault Status: r0p0, r1p0, r1p1, r1p2, r2p0. Open.

Description

HN-F System Level Caches (SLC) and Snoop Filter (SF) Debug Reads with simultaneous coherent traffic or dynamic power retention transitions can cause a deadlock.

Configurations affected

Any configuration.

Conditions

This erratum occurs when one of the following conditions are met:

- Coherent transactions that require HN-F Snoop Filter allocation while performing SLC or SF debug read
- Dynamic retention mode is enabled while performing a SLC or SF debug read

Implications

A deadlock can occur if the conditions are met. Note that expected usage is performing the Debug Reads in the absence of traffic since traffic can change the state of the RAMs.

Workaround

Use the following workarounds to prevent a deadlock:

- Stop CPU (RN-F) and IO (RN-I) coherent traffic before issuing Debug Reads
- Disable Dynamic retention power transitions via por_hnf_ppu_pwpr.dyn_en = 1'b0 (reset value)

3114475
Transactions targeting the HN-D AXI interface might be stalled by a continuous stream of CMN configuration transactions

Status

Affects: CMN-650
Fault Type: Programmer CAT-C
Fault Status: Present in r0p0, r1p0, r1p1, r1p2, r2p0. Open.

Description

Transactions to a HN-D targeting the AXI interface might be stalled by a continuous stream of transactions targeting the CMN configuration space. This includes CMN configuration registers and transactions targeting the CMN AXU interfaces.

Configurations affected

All configurations.

Conditions

This erratum occurs if both the following conditions are met:

- Read or Write transactions targeting the HN-D AXI interface AND
- A continuous stream of transactions targeting CMN configuration space. Examples of a continuous stream of transactions are a single CPU issuing reads or writes in a continuous loop, or multiple CPUs issuing reads in a polling loop, resulting in multiple outstanding transactions active in the HN-D continuously.

Implications

If the conditions are met, software that accesses CMN configuration space, including AXU interfaces, can create a denial-of-service scenario. This prevents transactions targeting the HN-D AXI interface from making progress.

Workaround

To prevent a continuous stream of transactions at the HN-D from occurring, serialize accesses to the CMN configuration space. For example, use polling loops to limit the number of CPUs accessing the CMN configuration space.