Parity Errors Troubleshooting Guide

Document ID: 116135

Contributed by Shawn Wargo, Cisco Engineering.
Jul 15, 2013

Contents

Introduction

This document describes soft and hard parity errors, explains common error messages, and recommends methods that help you avoid or minimize parity errors. Recent improvements in hardware and software design reduce parity problems as well.

Background

What is a processor or memory parity error?

Parity checking is the storage of an extra binary digit (bit) in order to represent the parity (odd or even) of a small amount of computer data (typically one byte) while that data is stored in memory. The parity value calculated from the stored data is then compared to the final parity value. If these two values differ, this indicates a data error, and at least one bit must have been changed due to data corruption.

Within a computer system, electrical or magnetic interference from internal or external causes can cause a single bit of memory to spontaneously flip to the opposite state. This event makes the original data bits invalid and is known as a parity error.

Such memory errors, if undetected, may have undetectable and inconsequential results or may cause permanent corruption of stored data or a machine crash.

There are many causes of memory parity errors, which are classified as either soft parity errors or hard parity errors.

Soft Errors

Most parity errors are caused by electrostatic or magnetic-related environmental conditions.

The majority of single-event errors in memory chips are caused by background radiation (such as neutrons from cosmic rays), electromagnetic interference (EMI), or electrostatic discharge (ESD). These events may randomly change the electrical state of one or more memory cells or may interfere with the circuitry used to read and write memory cells.

Known as soft parity errors, these events are typically transient or random and usually occur once. Soft errors can be minor or severe:

- Minor soft errors that can be corrected without component reset are single event upsets (SEUs).
- Severe soft errors that require a component or system reset are single event latchups (SELs).

Soft errors are not caused by hardware malfunction; they are transient and infrequent, are mostly likely a SEU, and are caused by an environmental disruption of the memory data.

If you encounter soft parity errors, analyze recent environmental changes that have occurred at the location of the affected system. Common sources of ESD and EMI that may cause soft parity errors include:

- Power cables and supplies
- Power distribution units
- Universal power supplies
- Lighting systems
- Power generators
- Nuclear facilities (radiation)
- Solar flares (radiation)

Hard Errors

Other parity errors are caused by a physical malfunction of the memory hardware or by the circuitry used to read and write memory cells.

Hardware manufacturers take extensive measures to prevent and test for hardware defects. However, defects are still possible; for example, if any of the memory cells used to store data bits are malformed, they may be unable to hold a charge or may be more vulnerable to environmental conditions.

Similarly, while the memory itself may be operating normally, any physical or electrical damage to the circuitry used to read and write memory cells may also cause data bits to be changed during transfer, which results in a parity error.

Known as hard parity errors, these events are typically very frequent and repeated and occur whenever the affected memory or circuitry is used. The exact frequency depends on the extent of the malfunction and how frequently the damaged equipment is used.

Remember that hard parity errors are the result of a hardware malfunction and reoccur whenever the affected component is used.

If you encounter hard parity errors, analyze physical changes that have occurred at the location of the affected system. Common sources of hardware malfunction that may lead to hard parity errors include:

- Power surges (no ground)
- ESD
- Overheating or cooling
- Incorrect or partial installation
- Component incompatibility
- Manufacturing defect

Common Error Messages

The Cisco IOS® software provides a variety of parity error messages, which vary with the affected component and its relative impact on the system.

Processor

Cache error detected!
CP0_CAUSE (reg 13/0): 0x00000400
CPO_ECC (reg 26/0): 0x000000B3
CPO_BUSERRDPA (reg 26/1): 0x000000B3
CPO_CACHERI (reg 27/0): 0x20000000

Real cache error detected. System will be halted.

Error: Primary instr cache, fields: data,
Actual physical addr 0x00000000,
virtual address is imprecise.

Imprecise Data Parity Error

Explanation This is the result of a parity error within the Level 2 (L2) cache (static random-access memory, or SRAM) used by route processor (RP) or switch processor (SP) CPU of the Multilayer Switch Feature Card 3 (MSFC3).

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request a Return Material Authorization (RMA) in order to replace the Supervisor Engine, and mark the module for equipment failure analysis (EFA).

%SYSTEM_CONTROLLER-3-ERROR: Error condition detected: SYSAD_PARITY_ERROR

Explanation This is the result of a parity error in the system address (data bus) used by the In-Band Controller (IBC) of the MSFC3.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the Supervisor Engine, and mark the module for EFA.

%SYSTEM_CONTROLLER-3-ERROR: Error condition detected: TM_DATA_PARITY_ERROR

Explanation This is the result of a parity error in the table manager data used by the IBC of the MSFC3.

Recommendation

Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the Supervisor Engine, and mark the module for EFA.

%SYSTEM_CONTROLLER-3-ERROR: Error condition detected: TM_NPP_PARITY_ERROR

Explanation This is the result of a parity error in the table manager 'next page pointer' used by the IBC of the MSFC3.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the Supervisor Engine, and mark the module for EFA.

In Cisco IOS software versions between 12.1(8)E and 12.2(33)SXI3, the default behavior in response to SYSTEM_CONTROLLER-3-ERROR events was to reset the IBC and log an error message.

However, this corrective action resulted in some documented cases of the IBC (and thus, CPU) no longer being able to transmit or receive data. Thus, the behavior was changed in Cisco IOS software versions later than 12.2(33)SXI4 to log an error message and reset the system; refer to Cisco bug ID CSCtf51541.

Interrupt exception, CPU signal 20, PC = 0x[dec]

Explanation This is the result of a single-bit parity error in the CPU L2 cache (SRAM) used by the Cisco Catalyst 6700 Series modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the 6700 module, and mark the module for EFA.

In Cisco IOS software versions earlier than 12.2(33)SXI5, a software bug (Cisco bug ID CSCtj06411) would cause even single-bit parity errors to reset the 6700 module. This was resolved in Versions 12.2(33)SXI6 and 12.2(33)SXJ for Supervisor Engine 720 and in Version 15.0SY for Supervisor Engine 2T.

RAM

%SYSTEM_CONTROLLER-3-ERROR: Error condition detected: SYSDRAM_PARITY_ERROR

Explanation This is the result of an uncorrectable parity error in the synchronous DRAM (SDRAM) memory modules (DIMM) used by the MSFC3.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, clean and reseat the DIMM, and continue to monitor. If the error continues, request an RMA in order to replace or upgrade the DIMM.

%SYSTEM_CONTROLLER-3-COR_MEM_ERR: Correctable DRAM memory error. Count [dec], log [hex]

Explanation This is the result of a correctable parity error in the SDRAM (DIMM) used by the MSFC3.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, clean and reseat the DIMM, and continue to monitor. If the error continues, request an RMA in order to replace or upgrade the DIMM.

%MWAM-DFC[dec]-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred, A_BUS_L2_ERRORS: 0x10000, A_BUS_MEMIO_ERRORS: 0x0, A_SCD_BUS_ERR_STATUS: 0x80983000

Explanation This is the result of a single-bit parity error in the DRAM used by 6700 Series modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, clean and reseat the DIMM, and continue to monitor. If the error continues, request an RMA in order to replace or upgrade the DIMM.

%PM_SCP-SP-2-LCP_FW_ERR_INFORM: Module [dec] is experiencing the following error: LTL Parity error detected on Coil #[dec].

Explanation This is the result of a parity error in the SRAM used by the Cisco Catalyst 6100 and Cisco Catalyst 6300 Series modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the 6100 or 6300 module, and mark the module for EFA.

%SYS-4-SYS_LCPERR4: Module [dec]: LTL Parity error detected on Coil #[dec]

Explanation This is the result of a parity error in the SRAM used by the 6100 and 6300 Series modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the 6100 or 6300 module, and mark the module for EFA.

ASIC

%PM_SCP-SP-2-LCP_FW_ERR_INFORM: Module [dec] is experiencing the following error: Port ASIC ([name]) packet buffer failure detected on ports [dec]

Explanation This is the result of a parity error in the port ASIC packet buffer (SRAM) used by the Cisco Catalyst 6148A Series Ethernet modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the 6148A module, and mark the module for EFA.

%LTL-SP-2-LTL_PARITY_CHECK: LTL parity check request for 0x[hex]

Explanation This is the result of a parity error in the port ASIC port index table (SRAM) used by the Catalyst 6100-6500 and 6700 Series modules.

Recommendation Monitor the system regularly for reoccurrence. If no further events are observed, it is a soft error. If the error occurs frequently, request an RMA in order to replace the module, and mark the module for EFA.

Refer to these Cisco IOS software documents for a comprehensive list of error messages:

- Cisco IOS Release 12.2SX System Message Guide
- Cisco IOS Release 15.x SY System Message Guide

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Latest Advancements

Research into the field of parity errors is ongoing, and not every scenario can be addressed, but the Cisco Catalyst 6500 hardware and software development organizations continue to introduce new ways, such as error-correcting code (ECC) protection, to minimize and mitigate the occurrence of parity errors.

While this document began with discussion of the third generation (WS-XSUP720 and early 6700 Series) of Catalyst 6500 products, this section summarizes improvements introduced with the fourth generation (VS-S720-10G and later 6700 Series) and the fifth generation (VS-SUP2T-10G and 6900 Series).

Processor

The VS-S720-10G module features a newer MSFC3 daughterboard, with a new IBC and updated SR7010A reduced instruction set computing (RISC) RP and SP CPUs that operate at 600Mhz each. The Level 1 (L1), L2, and Level 3 (L3) caches are capable of parity detection. The newer IBC has all of the functionality of the earlier generation and adds ECC protection (single-bit correction, multi-bit detection) to the attached SRAMs.

The 6700 Series modules support a CPU with ECC-protected L2 cache (L1 cache is parity detection capable), which can correct single-bit parity errors without the need to reset. However, due to Cisco bug ID CSCsz39222, Version 12.2SXI of the Cisco IOS software (Supervisor Engine 720) resets the module anyway if a single-bit CPU cache parity error occurs. This is resolved in Versions 12.2SXJ (Supervisor Engine 720) and 15.0SY (Supervisor Engine 2T) of the Cisco IOS software.

The VS-SUP2T-10G features a new MSFC5 daughterboard with an integrated IBC and a new single, dual-core MPC8572 PPC RP CPU (with ECC-protected L2 and L3 cache, L1 cache is parity detection capable) that operates at 1.5Ghz per core. It also features a new, separate, out-of-band Connectivity Management Processor (CMP) CPU and ECC-protected DRAM, which is available even if the RP CPU is currently unavailable.

The new IBC has all of the functionality of earlier generations and supports ECC protection for the attached SRAMs and improvements in parity error handling. The new MSFC5 also features an Onboard Failure Logging (OBFL) ROM, which stores all module initialization and diagnostics events. The new single CPU design also reduces the statistical likelihood of parity error events.

The 6900 Series modules support a newer CPU with ECC-protected L1 and L2 cache, which can correct single-bit parity errors without the need to reset. The new generation supports the same IBC, and the software handling for single-bit parity error correction has been incorporated.

RAM

The VS-S720-10G with MSFC3 features double-data-rate (DDR) SDRAM with ECC protection, operating at 266Mhz.

The 6700 Series modules support DDR SDRAM with ECC protection, operating at 266Mhz.

Compared to single-data-rate (SDR) SDRAM, the DDR SDRAM interface makes higher transfer rates possible by more strict control of the timing of the electrical data and clock signals. The DDR interface uses double pumping (data transfer on both the rising and falling edges of the clock signal) in order to lower the clock frequency. Lower clock frequency reduces the signal integrity requirements on the circuit board that connects the memory to the controller.

The VS-SUP2T-10G with MSFC5 features DDR3 SDRAM with ECC protection, operating at 667Mhz.

The 6900 Series modules support DDR3 SDRAM with ECC protection, operating at 667Mhz.

The primary benefit of DDR3 SDRAM over its immediate predecessors (DDR2 and DDR) is its ability to transfer data at twice the rate (eight times the speed of its internal memory arrays), which enables higher bandwidth or peak data rates. DDR3 memory also reduces power consumption by 30%, even though it uses the same electric signaling standard as DDR and DDR2.

ASIC

The VS-S720-10G with PFC3C features SRAM packet buffers with ECC protection. This provides single-bit parity error correction without module reset, as well as multi-bit parity error detection.

The 6700 Series with DFC3C features SRAM packet buffers with ECC protection. This provides single-bit parity error correction without module reset, as well as multi-bit parity error detection.

The VS-SUP2T-10G with PFC4 features SRAM packet buffers with ECC protection. This provides single-bit parity error correction without module reset, as well as multi-bit parity error detection.

The 6900 Series with DFC4 features SRAM packet buffers with ECC protection. This provides single-bit parity error correction without module reset, as well as multi-bit parity error detection.

Software

The Cisco IOS software is designed to support ECC protection. If a hardware component that supports ECC protection experiences an SEU, the code should correct the corrupt data or reset the affected component and not require a full hardware reset of the affected module.

However, in earlier versions of Cisco IOS software, there are a few exceptions where the behavior has been intentionally changed or malfunctions due to a software bug. Here are two notable exceptions.

MSFC IBC Reset

In Cisco IOS software versions between 12.1(8)E and 12.2(33)SXI3, the default behavior in response to SEU SYSTEM_CONTROLLER-3-ERROR events was to reset the IBC and log an error message. However, this corrective action resulted in some documented cases of the IBC (and thus, CPU) no longer being able to transmit or receive data.

Thus, the behavior was changed after Version 12.2(33)SXI4 (Cisco bug ID CSCtf51541) to log an error message and reset the system. While this reaction may seem more severe, it is preferable to reset the system and correct the memory structure than to have an unresponsive system.

A feature now in development (Cisco bug ID CSCtr89859) will add a new command-line interface (CLI) command that lets you switch the default behavior. This enhancement is most applicable to systems that use a single supervisor and thus have no supervisor redundancy.

6700 Series 'Single-Bit Parity Error' Reset

In Cisco IOS software versions earlier than12.2(33)SXI5, a software bug (Cisco bug ID CSCtj06411) would cause even single-bit parity errors to reset the 6700 module. This would normally be a correctable parity error and not require the module to be reset.

This bug was resolved in Versions 12.2(33)SXI6+ and 12.2SXJ for Supervisor Engine 720 and in Version 15.0SY for Supervisor Engine 2T. After an upgrade to the appropriate version, the 6700 module simply logs an error message and continues to operate.

Recommendations

By this point, you have probably determined whether you have encountered a soft or hard parity error. While this may address a single incident, other parity error vulnerabilities may still exist, so you should take a more comprehensive approach to your entire network.

Thus, Cisco and the Catalyst 6500 business unit recommend that you review these mitigation procedures and take appropriate corrective actions in order to eliminate or reduce future parity errors.

Soft Errors (SEU)

Single event (soft) parity errors are caused by environmental conditions and may occur only once (SEU) or very infrequently, such as monthly or yearly. Although you do not need to replace the hardware, you do want to mitigate future occurrences.

These best practices significantly reduce the likelihood of soft parity errors.

Environmental Audit

Cisco recommends that you perform an environmental audit of your affected network locations. You may perform this audit yourself or in coordination with a Cisco representative, with a Cisco team (such as Cisco Advanced Services), or through a third-party consultant.

The exact coverage and complexity of an environmental audit depend on many different variables such as geographic location, building and room size and design, electrical design and layout, and other related factors.

Consider what environmental sources of ESD and EMI may exist in or around your network. These are common sources of interference that may lead to a soft parity error:

- Power cables and supplies
- Power distribution units
- Universal power supplies
- Lighting systems
- Power generators
- Nuclear facilities (radiation)
- Solar flares (radiation)

Chassis Placement

SEUs can occur if power distribution units, power generators, or lighting systems are too close to the chassis or if multiple power cables are on or beside the chassis.

It is important to provide adequate distance between the Catalyst 6500 chassis and these electrical and magnetic sources. Recommended distances vary by component and are available from the component datasheets.

In general, Cisco recommends you locate systems at least three to six inches from common sources of electrical and magnetic interference. Power cables should be routed down and away from the chassis, wherever possible, and should not be laid in tightly packed bundles or in large numbers across or beside the chassis.

Grounding

Power fluctuations and power surges are relatively common, and Catalyst 6500 power supplies are designed to accommodate minor variations in voltage current.

However, it is critical to provide proper electrical grounding for the chassis and rack so any excess electrical voltage is drawn away from the system. Without proper grounding, power surges may result in damage or malfunction in various ASICs and memory components. Refer to the Catalyst 6500 Series Switch Installation Guide, Installing the Switch, Establishing the System Ground, for more information.

ESD

ESD can easily damage critical components without any visible impairment. Appropriate preventive measures should be incorporated into lab operation policies, but such measures are often and unfortunately ignored due to expedience and limited oversight.

Cisco recommends that your lab operations management, along with Cisco Systems, perform an environmental audit of all network areas or, at a minimum, of all areas that have exhibited hardware failures or have been designated as mission critical. Once the audit is complete, Cisco recommends that you implement a standardized environmental checklist for all newly installed systems in order to avoid future SEU parity events.

Latest Firmware (Rommon)

Catalyst hardware components use firmware (also known as Rommon) code to initialize, communicate, and run diagnostics. Once these functions are complete, system operation is turned over to the Cisco IOS software. It is uncommon to experience issues with firmware, but there can be issues if you use different versions of firmware code for the Supervisors and the modules.

Thus, it is a best practice to ensure that all components use the latest firmware code in order to ensure proper module initialization and communication. Cisco recommends that your operations management perform a network audit and upgrade all hardware components with the latest firmware version.

Known firmware issues and upgrade procedures are documented in:

- Release Notes for Supervisor Engine 720 Switch Processor ROMMON
- Release Notes for 6700 Series Switching Module ROMMON

Download the latest firmware versions from the Cisco web site:

- Cisco Catalyst 6500 Series Supervisor Engine 720 / MSFC3 - 8.5(4) Rommon
- Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10GE Uplinks - 12.2(18r)S1 Rommon

Thumb Screws

All modular networking systems are designed to insert into a chassis backplane with a set of physical interface pins. The chassis backplane itself is essentially a series of interconnected wires. The pins in each chassis slot form the physical data connection between the Supervisor and Ethernet modules. Thus, proper insertion and alignment of these pins is critical.

The Catalyst 6500 provides guide rails and alignment pins that assist in the installation in the chassis. The slot pins (sockets) and module connectors are designed to easily engage and provide high-bandwidth capable electrical connectivity. Once inserted into the chassis, there are thumb screws on either side of the module that fully engage the backplane pins. Refer to the Catalyst 6500 Series Switch Module Installation Note.

If a module has been properly inserted into the slot and the thumb screws have been correctly tightened, no communication problems are expected. However, several conditions may occur in day-to-day insertion of modules that can lead to improper or even incomplete pin insertion:

- **Insufficient insertion force** - If the module is partially inserted without use of the thumb screws, this may cause bus stalls, and the module may not be able to communicate with other modules. Depending on the level of insertion (for example, if there is limited physical contact), the module may be able to transmit and receive data, but may experience bit errors that result in corrupt packets.

- **Vertical misalignment** - This occurs when only one side of the module is on the guide rails. This is easily identified because the module appears diagonal and does not usually connect with the backplane pins.
- **Horizontal misalignment** - If thumb screws are used on only one side, some of the pins do not engage properly. This is a common problem, because the module may appear to be properly inserted. Horizontal misalignment is actually a form of insufficient insertion force.

Cisco recommends that you implement an operation management process that mandates the use of the thumb screws on all Catalyst 6500 modules in production environments. This ensures proper and full insertion and alignment of backplane pins and prevents future failures due to bit errors and related communication failures.

Hard Errors (Malfunction)

Frequent or repeatable (hard) parity errors are caused by physical malfunction of the memory or the circuitry used to read and write. In such cases, replace the hardware and ask the Cisco Technical Assistance Center (TAC) or your Cisco Systems Engineer to conduct an EFA on the returned hardware.

These best practices significantly reduce the likelihood of hard parity errors.

Hardware (MTBF and EOL) Audit

Cisco recommends that you perform a network audit of your affected network locations. You may perform this audit yourself or in coordination with a Cisco representative, with a Cisco team (such as Cisco Advanced Services), or through a third-party consultant.

All hardware (from all vendors) is subject to eventual degradation of physical integrity, and it is important to track the life cycle of all hardware components in your network in order to fully understand the likelihood of component failure over time.

Hardware reliability can be measured with the mean time between failure (MTBF) framework. Since MTBF is only a statistical average, this does not mean that a failure will definitely occur at the end of the MTBF time period. However, the likelihood and vulnerability of component failure increases, so such hardware should be flagged for refresh. Refer to the Cisco Catalyst 6500 Series Switches Data Sheets for specific MTBF values for each Catalyst 6500 product.

The aggregated calculated Catalyst 6500 'system-level' MTBF value is $\geq$ 7 years.

In addition to the MTBF framework, Cisco also provides an end-of-life (EOL) framework, which defines the expected life cycle of a given product and provides applicable announcements in order to help you refresh your legacy equipment. Refer to the End-of-Life and End-of-Sale Notices for various legacy Catalyst 6500 products.

As a result of this hardware audit, Cisco recommends that you implement your own MTBF and EOL process that identifies and tracks hardware for potential refresh. This ensures that the latest hardware is running and minimizes the likelihood of hardware malfunction.

Hardware Diagnostics

The Catalyst 6500 Series and Cisco IOS software provides Generic Online Diagnostics (GOLD) and Health Monitoring (HM) diagnostics for all hardware components used in the system. The two basic types of diagnostics that can be enabled are on-demand and boot-up. Refer to Generic Online Diagnostics on the Cisco Catalyst 6500 Series Switch for additional information.

Cisco recommends that 'complete' boot-up diagnostics be enabled for all hardware components in order to ensure that all diagnostic tests are executed and to confirm that all hardware components are functioning as expected upon boot-up.

Cisco also recommends that you schedule regular, on-demand diagnostics of critical infrastructure components on a daily or weekly basis. Beyond the boot-up diagnostics that occur only during initialization, the on-demand diagnostics ensure that the hardware continues to operate as expected. Refer to Catalyst 6500 Release 12.2SX Software Configuration Guide, Interface and Hardware Components, Online Diagnostics for more information.

In addition to the default on-demand diagnostic tests, Cisco recommends that you enable these on-demand diagnostic tests in order to proactively identify memory components that might malfunction:

- TestLinecardMemory
- TestAsicMemory

Updated: Jul 15, 2013 Document ID: 116135