

# Cisco MDS 9000 Series High Availability Configuration Guide, Release 9.x

**First Published:** 2022-09-02

**Last Modified:** 2026-03-05

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



# CONTENTS


**Full Cisco Trademarks with Software License** ?

PREFACE

**Preface** v

Audience v

Document Conventions v

Documentation Feedback vii

Related Documentation vii

Communications, Services, and Additional Information vii

CHAPTER 1

**New and Changed Information** 1

CHAPTER 2

**High Availability Overview** 5

Supervisor Redundancy 5

Internal CRC Detection and Isolation 6

Stages of Internal CRC Detection and Isolation 7

Actions Taken on a Supervisor when the Threshold Exceeded 9

CHAPTER 3

**Configuring High Availability** 11

Finding Feature Information 11

Feature History for High Availability 11

Configuring High Availability 12

About High Availability 12

Switchover Processes 13

Synchronizing Supervisor Modules 13

Manual Switchover Guidelines 13

Manually Initiating a Switchover 14

Configuring Internal CRC Detection and Isolation 15
Default Settings for Internal CRC Detection and Isolation 15
Copying Boot Variable Images to the Standby Supervisor Module 15
Enabling Automatic Copying of Boot Variables 16
Verifying the Copied Boot Variables 16
Displaying HA Status Information 17
Displaying the System Uptime 19

CHAPTER 4 **Fabric Module Error Monitoring** 21
Feature History for Fabric Module Error Monitoring 21
About Fabric Module Error Monitoring 21
Guidelines and Limitations of Fabric Module Error Monitoring 22
Default Values 23
Configuring Fabric Module Error Monitoring 25
Alerting for Fabric Module Error Monitoring 25
Configuration Examples 26



# Preface

This preface describes the audience, organization of, and conventions used in the Cisco MDS 9000 Series Configuration Guides. It also provides information on how to obtain related documentation, and contains the following sections:


- Audience, on page v
- Document Conventions, on page v
- Documentation Feedback, on page vii
- Related Documentation, on page vii
- Communications, Services, and Additional Information, on page vii


## Audience

This publication is for network administrators who install, configure, and maintain Cisco MDS 9000 Series Switches.

## Document Conventions

Command descriptions use these conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates the commands and keywords that you enter literally as shown. |
| *Italic* | Italic text indicates arguments for which the user supplies the values. |
| [x] | Square brackets enclose an optional element (keyword or argument). |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice. |
| {x \| y} | Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice. |

| Convention | Description |
|---|---|
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| `variable` | Indicates a variable for which you supply values, in context where italics cannot be used. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |

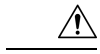
Examples use these conventions:

| Convention | Description |
|---|---|
| `screen font` | Terminal sessions and information the switch displays are in screen font. |
| **`boldface screen font`** | Information you must enter is in boldface screen font. |
| *italic screen font* | Arguments for which you supply values are in italic screen font. |
| < > | Nonprinting characters, such as passwords, are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

This document uses the following conventions:



**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



**Warning** IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

# Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to mds-docfeedback@cisco.com. We appreciate your feedback.

# Related Documentation

The entire Cisco MDS 9000 Series switches documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/series.html

Documentation Roadmap

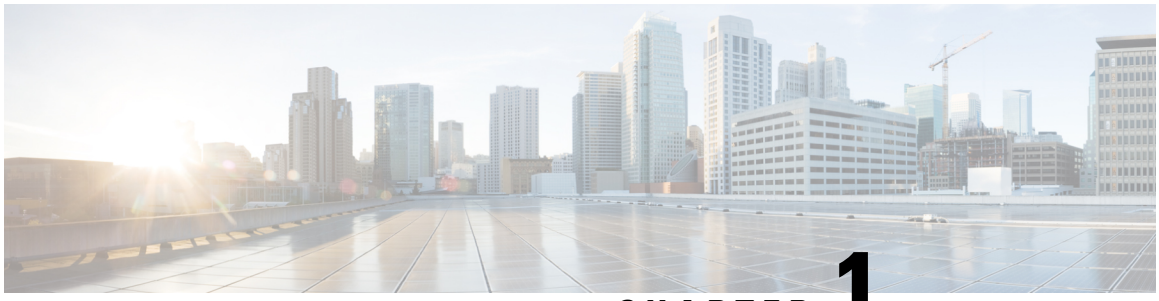
https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

# New and Changed Information

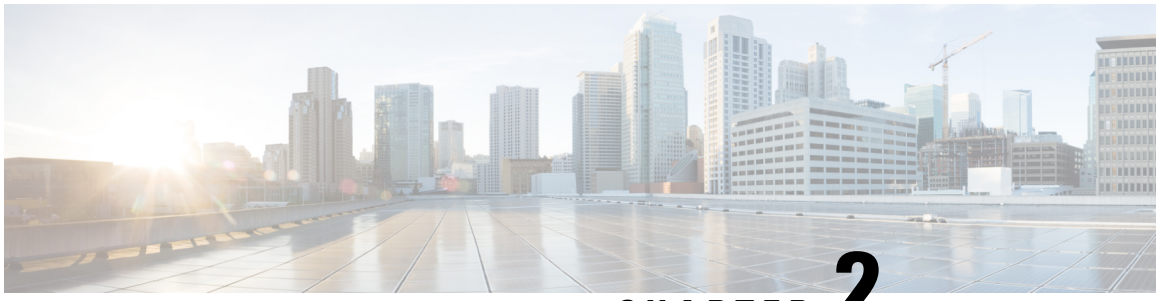
This table lists the New and Changed features.

***Table 1: New and Changed Features***

| Feature Name | Description | Release | Where Documented |
|---|---|---|---|
| FabricModule Error Monitoring | Support has been introduced for new error counters by default in Fabric Module Error Monitoring feature. They are the "HIGH_NULL_FCE_DROP_CNT" counter for Fabric 1 Modules and the "null FPOE port" counter for Fabric 3 Modules. The default error threshold has been changed from 50 to 10 errors per monitoring interval. | 9.4(5) | Fabric Module Error Monitoring |

| Feature Name | Description | Release | Where Documented |
|---|---|---|---|
| Standby Supervisor's mgmt0 Status | A syslog was introduced to alert the user if the standby supervisor's Ethernet management port is disconnected or down before performing an ISSU or system switchover.<br><br>The **show interface mgmt** *number* **standby** command was introduced to display the status of the supervisor's mgmt0 link when issued from the active supervisor.<br><br>The **system switchover bypass-standby-mgmt0** command was introduced to skip checking for the status of the standby supervisor's mgmt0 link during a system switchover. | 9.2(1) | Configuring High Availability, on page 11 |
| Internal CRC detection and error logging | Internal CRC detection and error logging without isolation is enabled by default. | 8.5(1) | Configuring High Availability, on page 11 |
| Internal CRC detection and error logging | An option to log internal CRC errors without taking any isolation action was introduced. | 8.4(2) | **hardware fabric crc** command in Cisco MDS 9000 Series Command Reference. |
| Standby Supervisor's mgmt0 Link | The standby supervisor's management Ethernet link on Cisco MDS Director switches is brought up when the supervisor reaches the standby state. | 8.4(2) | Configuring High Availability, on page 11 |

| Feature Name | Description | Release | Where Documented |
|---|---|---|---|
| Internal CRC Detection and Isolation | An option to log internal CRC errors without taking any action was added. | 8.4(2) | Configuring High Availability, on page 11 |



CHAPTER 2

# High Availability Overview

You can configure the high availability (HA) software framework and redundancy features using CLI. These features include application restartability and nondisruptive supervisor switchability. Cisco high availability is a technology that is delivered in Cisco NX-OS software that enables networkwide resilience to increase network availability.

The Cisco MDS Multilayer Directors and switches support application restartability and nondisruptive supervisor switchability. The switches are protected from system failure by redundant hardware components and a high availability software framework.

The high availability software framework enables the following features:

- Ensures nondisruptive software upgrade capability.
- Provides redundancy for supervisor module failure by using dual supervisor modules.
- Performs nondisruptive restarts of failed process on the same supervisor module. A service running on the supervisor and the switching modules tracks the high availability policy that is defined in the configuration and takes action based on the policy. This feature is also available in the Cisco MDS 9200 and MDS 9100 switches.
- Protects against a link failure using the port channel (port aggregation) feature. This feature is also available in the Cisco MDS 9200 and MDS 9100 switches.
- Provides switchovers when an active supervisor fails. The standby supervisor, if present, takes over without disrupting storage or host traffic.
- Enables the Cisco MDS switches to detect CRC errors that occur internally within a switch and isolate the source of the errors.


- Supervisor Redundancy, on page 5
- Internal CRC Detection and Isolation, on page 6


# Supervisor Redundancy

Cisco MDS Director switches have two supervisor modules for redundancy. When the switch powers up and both supervisor modules are present, the supervisor module that comes up first enters the active mode and the supervisor module that comes up second enters the standby mode. The supervisor in active mode is in control of the switch. It performs all the necessary functions to ensure that all the switch's components are operating normally. The standby supervisor module constantly monitors the active supervisor module. If the

active supervisor module fails, the standby supervisor module takes over without any impact to the user traffic. If the failed supervisor recovers, it will become the standby supervisor and monitors the new active supervisor.

Prior to Cisco MDS NX-OS Release 8.4(2), the standby supervisor's management Ethernet link on Cisco MDS Director switches was down. Therefore, the peer port of the management link was also down and could be mistaken as an unused port. This unused port could either be mistakenly disabled or repurposed. If a switchover occurred, the management link on the newly active supervisor would not be available and the switch would become unmanageable because there would be no active connection to the newly active supervisor's management port.

From Cisco MDS NX-OS Release 8.4(2), the standby supervisor's management Ethernet link on Cisco MDS Director switches is brought up when the supervisor reaches the standby state. However, no upper layer protocols, such as IP, are active. This allows the peer port of the standby supervisor's management link to be up and not mistakenly disabled or repurposed due to being down for a long duration.



**Note** For out of band management with high availability in director switches, you must connect the *mgmt0* port of both supervisors to the same subnet or virtual LAN since the mgmt0 IP address will be used by whichever supervisor is currently active.

# Internal CRC Detection and Isolation

Beginning with the Cisco MDS NX-OS Release 6.2(13), the Internal Cyclic Redundancy Check (CRC) detection and isolation functionality is supported on the Cisco MDS 9700 series switches.

This functionality enables the Cisco MDS switches to detect CRC errors that occur internally within a switch and isolate the source of these errors.



**Note** Internal CRC Detection and Isolation is supported only on the Cisco MDS 9700 Series Multilayer Directors.

From NX-OS Release 8.5(1) and Release 9.2(1), the internal CRC detection and isolation feature is enabled, by default, to log instances of 3 internal CRC errors per 24-hour period without taking any action.

The modules that support this functionality are:

- Cisco MDS 9700 48-Port 64-Gbps Fibre Channel Switching Module
- Cisco MDS 9700 48-Port 16-Gbps Fibre Channel Switching Module
- Cisco MDS 9700 48-Port 10-Gbps Fibre Channel over Ethernet Switching Module
- Cisco MDS 9700 40-Gbps 24-Port Fibre Channel over Ethernet Switching Module
- Cisco MDS 24/10-Port SAN Extension Switching Module
- Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module
- Cisco MDS 9700 Fabric Module 1
- Cisco MDS 9700 Fabric Module 3
- Cisco MDS 9700 Supervisor Module 1

- Cisco MDS 9700 Supervisor Module 4

**Note** *Module* refers either a switching module or a supervisor module.

These internal CRC errors are a separate class of CRC errors when compared to frames that arrive from outside the switch, with CRC errors. Frames that arrive from outside the switch on links are checked at ingress. If a frame does not pass the ingress CRC check it is dropped at the ingress port and does not propagate through the system. MDS switches including MDS 9700 directors operate in store and forward mode. Internal CRC errors occur when frames are received without errors, but get corrupted when they pass through the switching path. This corruption can occur in 5 'stages' in the forwarding path.

Internal CRC errors are usually caused by a fault in the system. Such faults may be transient, such as an ungracefully removed module, or permanent, such as a badly seated module, or, in rare cases, a failing or failed hardware component. The rate of errors depends on many factors and may range from very high to very low.

The error-rate threshold is configurable as a system-wide value, but separate error counts are maintained for each ASIC on each module to identify an error source.

When an ASIC involved in frame forwarding receives a frame it is CRC checked. If the CRC check does not pass then normally it is the receiving ASIC that is the faulty ASIC. However, it is possible that it was corrupted and sent incorrectly by the transmitting ASIC or corrupted along the link between the two ASICs. Depending on which ASIC or other component is at fault the errors may isolated to the single ASIC or they may be occurring on multiple ASICs if, for example, a faulty ASIC is transmitting to multiple receiving ASICs. Determining the faulty component involves understanding the multiple stages and looking at all of the internal CRC errors that are occurring.

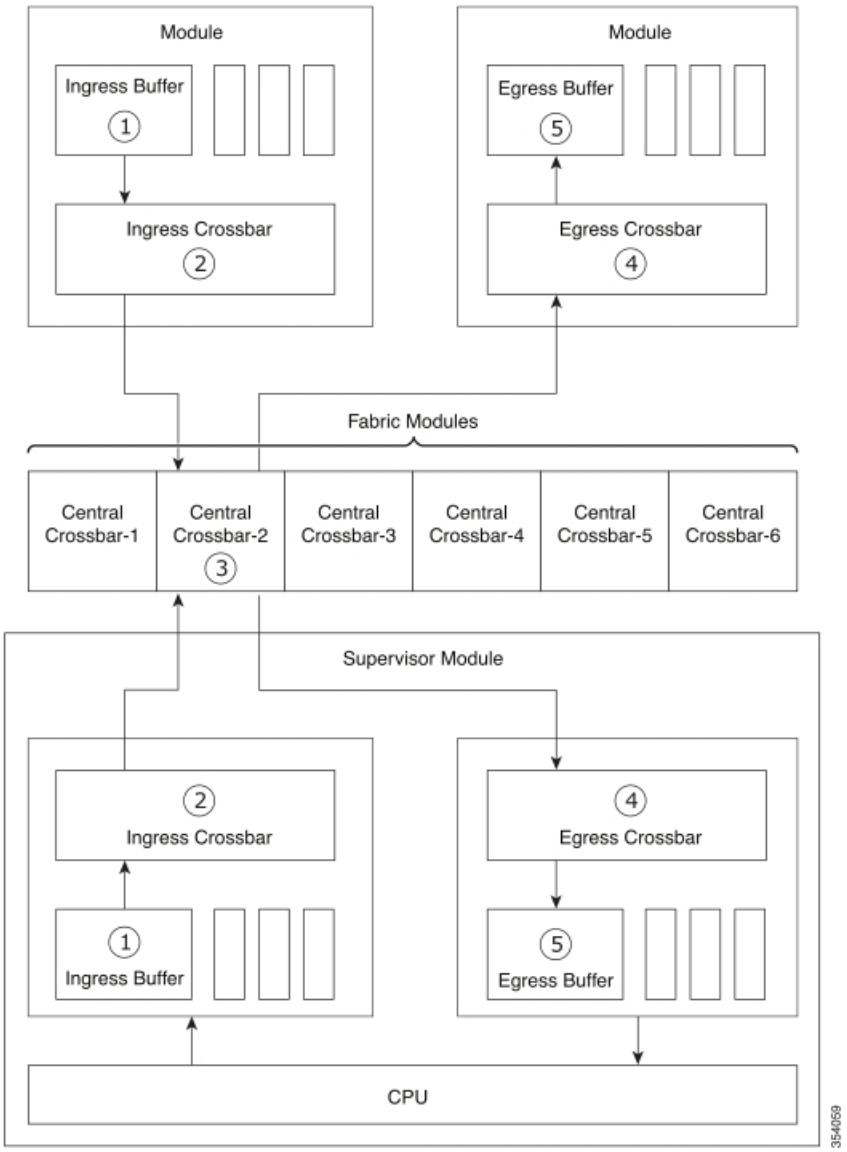
**Note** The counters are reset at 24 hours from the time the feature, the Internal Cyclic Redundancy Check (CRC) detection and isolation was first configured.

# Stages of Internal CRC Detection and Isolation

The five possible stages at which internal CRC errors may occur in a switch:

1. **Stage 1**—Ingress Buffer of a Module
2. **Stage 2**—Ingress Crossbar of a Module
3. **Stage 3**—Central Crossbar of a Chassis
4. **Stage 4**—Egress crossbar of a Module
5. **Stage 5**—Egress Buffer of a Module

*Figure 1: Stages of Internal CRC Detection and Isolation*




Errors on each module are handled individually when the error count exceeds the threshold.

**Note** A total of errors on all applicable ASICs on the module must exceed the threshold.

When errors cross the specified threshold, XBAR_MONITOR_INTERNAL_CRC_ERR is the syslog message that is logged. This syslog message specifies the location of the error and the type of action taken.

**Example:** Error Messages

```
switch# show logging logfile | inc MONITOR_INTERNAL_CRC_ERR
2015 May 25 21:20:41 switch %XBAR-2-XBAR_MONITOR_INTERNAL_CRC_ERR: Module-1 detects CRC
```

```
Error:4 at Egress Q-engine, putting it in failure state
2015 May 25 21:15:35 switch %XBAR-2-XBAR_MONITOR_INTERNAL_CRC_ERR: Fab_slot-12 detects CRC
error:1 at ingress stage2, putting it in failure state
2015 May 25 15:47:10 switch %XBAR-2-XBAR_MONITOR_INTERNAL_CRC_ERR: Module-5 detects CRC
error:2 at Ingress Qengine, Only one Sup is present, bringing down the active VSAN
2015 May 25 15:08:17 switch %XBAR-2-XBAR_MONITOR_INTERNAL_CRC_ERR: Module-5 detects CRC
error:1 at Ingress Qengine, putting it in failure state
```

**Stage 1—Ingress Buffer of a Module**

There are multiple ingress buffers on each module. When the CRC error rate of an ingress buffer on a switching module reaches the threshold, the entire module is shut down. See Actions Taken on a Supervisor when the Threshold Exceeded for more information.

**Stage 2—Ingress Crossbar of a Module**

Ingress crossbar is an ASIC complex on an ingress module that switches traffic from ingress buffers to fabric modules. When the CRC error rate of an ingress switching module crossbar reaches the threshold, the entire module is shut down. See Actions Taken on a Supervisor when the Threshold Exceeded for more information.

**Stage 3—Central Crossbar of a Chassis**

Crossbar is an ASIC complex on a fabric module that switches traffic from an ingress module to an egress module.

When the CRC error rate of a crossbar reaches the threshold, if there is more than one fabric module in the corresponding switch, the fabric module recording the errors is shut down. If the switch has only one fabric module, the module connected to the fabric module link on which the errors occurred is shut down.

**Stage 4—Egress Crossbar of a Module**

Egress crossbar is an ASIC complex on an egress module that switches traffic from fabric modules to egress buffers. When the CRC error rate of an egress switching module crossbar reaches the threshold, the connected central crossbar where the frame that has an error was received is powered down. See Actions Taken on a Supervisor when the Threshold Exceeded for more information.

**Stage 5—Egress Buffer of a Module**

There are multiple egress buffers on each module. When the CRC error rate of an egress buffer on a switching module reaches the threshold, the entire module is shut down. See Actions Taken on a Supervisor when the Threshold Exceeded for more information.

## Actions Taken on a Supervisor when the Threshold Exceeded

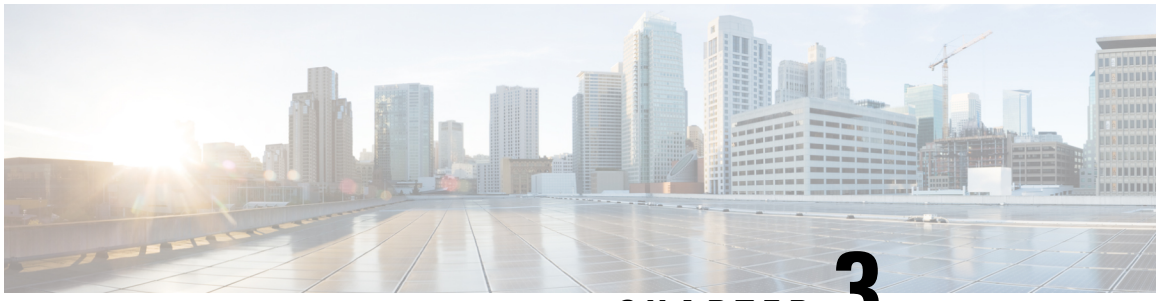
The actions taken on a supervisor when the threshold is exceeded during the following stages of internal CRC detection and isolation:

1. **Stage 1**—Ingress Buffer of a Module
2. **Stage 2**—Ingress Crossbar of a Module
3. **Stage 4**—Egress Crossbar of a Module
4. **Stage 5**—Egress Buffer of a Module

**Note**

- When both active and standby supervisors are present in the switch, the active supervisor is brought down and the standby takes over.
- When only active supervisor is present in the switch (second supervisor is absent or down), all active VSANs are suspended so that the data traffic stops. The active supervisor is available for manual debugging.
- When both a single fabric module is present and and a single supervisor module is present and Stage 2 errors occur on the supervisor, the supervisor is powered down; as a result the switch is brought down.

For information on configuring the Internal CRC Detection and Isolation feature, see Configuring Internal CRC Detection and Isolation, on page 15.



CHAPTER 3

# Configuring High Availability

This chapter describes how to configure high availability, and describes the switchover processes.


- Finding Feature Information, on page 11
- Feature History for High Availability, on page 11
- Configuring High Availability, on page 12


## Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://bst.cloudapps.cisco.com/bugsearch and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

## Feature History for High Availability

This table lists the New and Changed features.

*Table 2: New and Changed Features*

| Feature Name | Release | Feature Information |
|---|---|---|
| Standby Supervisor’s mgmt0 Status | 9.2(1) | A syslog was introduced to alert the user if the standby supervisor's Ethernet management port is disconnected or down before performing an ISSU or system switchover.<br>The **show interface mgmt** *number* **standby** command was introduced to display the status of the supervisor's mgmt0 link when issued from the active supervisor.<br>The **system switchover bypass-standby-mgmt0** command was introduced to skip checking for the status of the standby supervisor's mgmt0 link during a system switchover. |
| Internal CRC Detection and Isolation | 8.5(1) | Internal CRC detection and error logging without isolation is enabled by default. |
| Standby Supervisor's mgmt0 Link | 8.4(2) | The standby supervisor's management Ethernet link on Cisco MDS Director switches is brought up when the supervisor reaches the standby state. |
| Internal CRC Detection and Isolation | 8.4(2) | Added an option to log internal CRC errors without taking any action.<br>The following command was modified:<br>**hardware fabric crc** [**threshold** *count*] [**log-only**] |

# Configuring High Availability

This chapter describes how to configure high availability, and describes the switchover processes.

## About High Availability

Process restartability provides the high availability functionality in Cisco MDS 9000 Series switches. This process ensures that process-level failures do not cause system-level failures. It also restarts the failed processes automatically. This process is able to restore its state prior to the failure and continues executing from the failure point going forward.

From Cisco MDS NX-OS Release 8.4(2), the standby supervisor's management Ethernet link on Cisco MDS Director switches is brought up when the supervisor reaches the standby state. This will help prevent the port in the adjacent Ethernet switch from being detected as continuously down and potentially decommissioned.

From Cisco MDS NX-OS Release 9.2(1), NX-OS checks and prints a syslog to alert the user if the standby supervisor's Ethernet management link is disconnected or down before performing an In-Service Software

Upgrade (ISSU), In-Service Software Downgrade (ISSD), or system switchover. You can also use the **show interface mgmt** *number* **standby** command to display the status of the standby supervisor's mgmt0 link when issued from the active supervisor. Use the **system switchover bypass-standby-mgmt0** command to skip checking for the status of the standby supervisor's mgmt0 link during a system switchover. For information on system messages, see the Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference.

An HA switchover has the following characteristics:

- It is stateful (nondisruptive) because control traffic is not impacted.
- It does not disrupt data traffic because the switching modules are not impacted.
- Switching modules are not reset.

**Note** Switchover is not allowed if **auto-copy** is in progress.

# Switchover Processes

Switchovers occur by one of the following two processes:

- The active supervisor module fails and the standby supervisor module automatically takes over.
- You manually initiate a switchover from an active supervisor module to a standby supervisor module.

Once a switchover process has started another switchover process cannot be started on the same switch until a stable standby supervisor module is available.

**Caution** If the standby supervisor module is not in a stable state (ha-standby), a switchover is not performed.

## Synchronizing Supervisor Modules

The running image is automatically synchronized in the standby supervisor module by the active supervisor module. The boot variables are synchronized during this process.

The standby supervisor module automatically synchronizes its image with the running image on the active supervisor module.

**Note** The image a supervisor module is booted up from cannot be deleted from bootflash. This is to ensure that the new standby supervisor module ia able to synchronize during the process.

## Manual Switchover Guidelines

Be aware of the following guidelines when performing a manual switchover:

- When you manually initiate a switchover, system messages indicate the presence of two supervisor modules.
- A switchover can only be performed when two supervisor modules are functioning in the switch.

- The modules in the chassis are functioning as designed.

## Manually Initiating a Switchover

To manually initiate a switchover from an active supervisor module to a standby supervisor module, use the **system switchover** command. After you enter this command, another switchover process cannot be started on the same switch until a stable standby supervisor module is available.

To ensure that an HA switchover is possible, enter the **show system redundancy status** command or the **show module** command. If the command output displays the HA standby state for the standby supervisor module, then the switchover is possible. See Verifying Switchover Possibilities for more information.

### Verifying Switchover Possibilities

This section describes how to verify the status of the switch and the modules before a manual switchover.

- Use the **show interface mgmt** *number* **standby** command to verify that the standby supervisor's mgmt0 link is up.
- Use the **show system redundancy status** command to ensure that the system is ready to accept a switchover.
- Use the **show module** command to verify the status (and presence) of a module at any time. A sample output of the **show module** command follows:

```
switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------------------ ------------------ ------------
2 8 IP Storage Services Module DS-X9308-SMIP ok
5 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
6 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 ha-standby
8 0 Caching Services Module DS-X9560-SMAP ok
9 32 1/2 Gbps FC Module DS-X9032 ok
Mod MAC-Address(es) Serial-Num
--- -------------------------------------- ----------
2 00-05-30-00-9d-d2 to 00-05-30-00-9d-de JAB064605a2
5 00-05-30-00-64-be to 00-05-30-00-64-c2 JAB06350B1R
6 00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd JAB06350B1R
8 00-05-30-01-37-7a to 00-05-30-01-37-fe JAB072705ja
9 00-05-30-00-2d-e2 to 00-05-30-00-2d-e6 JAB06280ae9
* this terminal session
```

The Status column in the output should display an OK status for switching modules and an active or HA-standby status for supervisor modules. If the status is either OK or active, you can continue with your configuration.

- Use the **show boot auto-copy** command to verify the configuration of the auto-copy feature and if an auto-copy to the standby supervisor module is in progress. Sample outputs of the **show boot auto-copy** command follow:

```
switch# show boot auto-copy
Auto-copy feature is enabled
switch# show boot auto-copy list
No file currently being auto-copied
```

## Configuring Internal CRC Detection and Isolation

**Note** This functionality is disabled by default.

To configure internal CRC detection and isolation, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# **configure terminal**

**Step 2** Enable internal CRC detection, isolation, and error logging:

switch(config)# **hardware fabric crc** [**threshold** *count*]

Or

Enable internal CRC detection and error logging without isolation in Cisco MDS NX-OS Release 8.4(2) and later releases:

switch(config)# **hardware fabric crc** [**threshold** *count*] **log-only**

From Cisco MDS NX-OS Release 8.5(1), internal CRC detection and error logging without isolation is enabled by default.

The error rate is measured over a sequential 24-hour window, where the error count is reset to 0 at the start of each window. The threshold range is 1–100. The default threshold is 3 when the threshold is not specified.

**Step 3** (Optional) Disable internal CRC detection, isolation, and error logging:

switch(config)# **no hardware fabric crc**

**Step 4** Save the configuration change:

switch(config)# **copy running-config startup-config**

## Default Settings for Internal CRC Detection and Isolation

The table below lists the default settings for interface parameters.

***Table 3: Default Settings for Internal CRC Detection and Isolation***

| Parameters | Default |
|---|---|
| Internal CRC Error Handling | Disabled |

# Copying Boot Variable Images to the Standby Supervisor Module

You can copy the boot variable images that are in the active supervisor module (but not in the standby supervisor module) to the standby supervisor module. Only those KICKSTART and SYSTEM boot variables that are

set for the standby supervisor module can be copied. For module (line card) images, all boot variables are copied to the corresponding standby locations (bootflash: or slot0:) if not already present.

## Enabling Automatic Copying of Boot Variables

To enable or disable automatic copying of boot variables, follow these steps:

### Procedure

**Step 1** Enters configuration mode.

switch# **configure terminal**

switch(configure)#

**Step 2** Enables (default) automatic copying of boot variables from the active supervisor module to the standby supervisor module.

switch(configure)# **boot auto-copy**

Auto-copy administratively enabled

**Step 3** Disables the automatic copy feature.

switch(configure)# **boot auto-copy**

Auto-copy administratively disabled

## Verifying the Copied Boot Variables

Use the **show boot auto-copy** command to verify the current state of the copied boot variables. This example output shows that automatic copying is enabled:

```
switch# show boot auto-copy
Auto-copy feature enabled
```

This example output shows that automatic copying is disabled:

```
switch# show boot auto-copy
Auto-copy feature disabled
```

Use the **show boot auto-copy list** command to verify what files are being copied. This example output displays the image being copied to the standby supervisor module's bootflash. Once this is successful, the next file will be image2.bin.



**Note** This command only displays files on the active supervisor module.

```
switch# show boot auto-copy list
File: /bootflash:/image1.bin
Bootvar: kickstart
```

```
File:/bootflash:/image2.bin
Bootvar: system
```

This example output displays a typical message when the **auto-copy** option is disabled or if no files are copied:

```
switch# show boot auto-copy list
No file currently being auto-copied
```

# Displaying HA Status Information

Use the **show system redundancy status** command to view the HA status of the system. Tables Redundancy States to Internal States Table 4: Redundancy States , on page 17 and Table 6: Internal States , on page 18 explain the possible output values for the redundancy, supervisor, and internal states.

```
switch# show system redundancy status
Redundancy mode
---------------
      administrative:   HA
         operational:   HA
This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with HA standby
Other supervisor (sup-2)
------------------------
    Redundancy state:   Standby
    Supervisor state:   HA standby
      Internal state:   HA standby
```

The following conditions identify when automatic synchronization is possible:

- If the internal state of one supervisor module is Active with HA standby and the other supervisor module is HA standby, the switch is operationally HA and can do automatic synchronization.
- If the internal state of one of the supervisor modules is none, the switch cannot do automatic synchronization.

The following table lists the possible values for the redundancy states.

***Table 4: Redundancy States***

| State | Description |
|---|---|
| Not present | The supervisor module is not present or is not plugged into the chassis. |
| Initializing | The diagnostics have passed and the configuration is being downloaded. |
| Active | The active supervisor module and the switch is ready to be configured. |
| Standby | A switchover is possible. |

| State | Description |
|---|---|
| Failed | The switch detects a supervisor module failure on initialization and automatically attempts to power-cycle the module three (3) times. After the third attempt it continues to display a failed state.<br>**Note**<br>You should try to initialize the supervisor module until it comes up as HA-standby. This state is a temporary state. |
| Offline | The supervisor module is intentionally shut down for debugging purposes. |
| At BIOS | The switch has established connection with the supervisor and the supervisor module is performing diagnostics. |
| Unknown | The switch is in an invalid state. If it persists, call TAC. |

The following table lists the possible values for the supervisor module states.

***Table 5: Supervisor States***

| State | Description |
|---|---|
| Active | The active supervisor module in the switch is ready to be configured. |
| HA standby | A switchover is possible. |
| Offline | The switch is intentionally shut down for debugging purposes. |
| Unknown | The switch is in an invalid state and requires a support call to TAC. |

The following table lists the possible values for the internal redundancy states.

***Table 6: Internal States***

| State | Description |
|---|---|
| HA standby | The HA switchover mechanism in the standby supervisor module is enabled (see the Synchronizing Supervisor Modules section). |
| Active with no standby | A switchover is not possible. |
| Active with HA standby | The active supervisor module in the switch is ready to be configured. The standby supervisor module is in the HA-standby state. |
| Shutting down | The switch is being shut down. |
| HA switchover in progress | The switch is in the process of changing over to the HA switchover mechanism. |
| Offline | The switch is intentionally shut down for debugging purposes. |
| HA synchronization in progress | The standby supervisor module is in the process of synchronizing its state with the active supervisor modules. |

| State | Description |
|---|---|
| Standby (failed) | The standby supervisor module is not functioning. |
| Active with failed standby | The active supervisor module and the second supervisor module is present but is not functioning. |
| Other | The switch is in a transient state. If it persists, call TAC. |

From Cisco MDS NX-OS Release 8.5(1), use the **show hardware fabric crc status** command to display the status of the internal CRC detection and isolation function.

```
switch# show hardware fabric crc status
Hardware Fabric CRC Action : log-only
Hardware Fabric CRC Feature threshold per module stage : 3
Hardware Fabric CRC Feature sampling time in hours : 24
```

# Displaying the System Uptime

The system uptime refers to the time that the chassis was powered on and has at least one supervisor module controlling the switch. Use the **reset** command to reinitialize the system uptime. On switches that use dual supervisors, nondisruptive upgrades and switchovers do not reinitialize the system uptime, which means that the system uptime is contiguous across such upgrades and switchovers.

The kernel uptime refers to the time since the NX-OS software was loaded on the supervisor module. Use the **reset** and **reload** commands to reinitialize the kernel uptime.

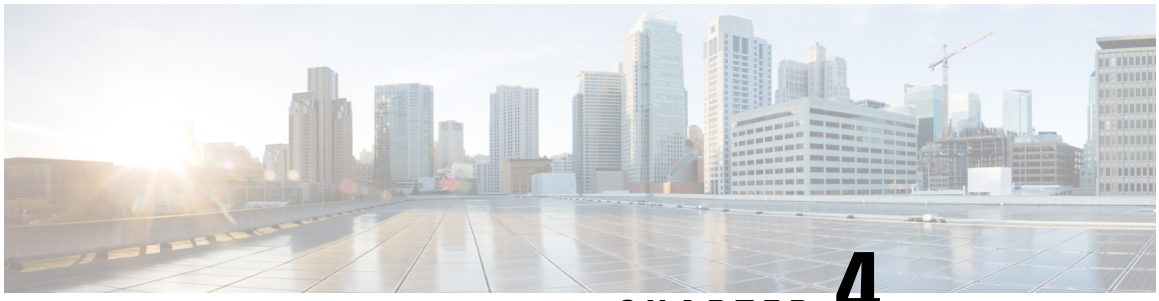
The active supervisor uptime refers to the time since the NX-OS software was loaded on the active supervisor module. The active supervisor uptime can be lower than the kernel uptime after nondisruptive switchovers.

You can use the **show system uptime** command to view the start time of the system, uptime of the kernel, and the active supervisor.

This example shows how to display the supervisor uptime:

```
switch# show system uptime
System start time:          Fri Aug 27 09:00:02 2004
System uptime:              1546 days, 2 hours, 59 minutes, 9 seconds
Kernel uptime:              117 days, 1 hours, 22 minutes, 40 seconds
Active supervisor uptime:   117 days, 0 hours, 30 minutes, 32 seconds
```

For more information on high availability, see chapter 1, High Availability Overview.



CHAPTER 4

# Fabric Module Error Monitoring

This chapter provides information about Fabric Module Error Monitoring and how to configure it.


- Feature History for Fabric Module Error Monitoring, on page 21
- About Fabric Module Error Monitoring, on page 21
- Guidelines and Limitations of Fabric Module Error Monitoring, on page 22
- Default Values, on page 23
- Configuring Fabric Module Error Monitoring, on page 25
- **Alerting for Fabric Module Error Monitoring**, on page 25
- Configuration Examples, on page 26


## Feature History for Fabric Module Error Monitoring

| Feature Name | Releases | Feature Information |
|---|---|---|
| Fabric Module Error Monitoring | 9.4(5) | The Fabric 1 **HIGH_NULL_POE_DROP_CNT** and Fabric 3 **null fpoe port** error counters were added. |
| Fabric Module Error Monitoring | 9.3(1) | This feature was introduced. |

## About Fabric Module Error Monitoring

The fabric modules of modular Cisco MDS platforms are commonly called Xbars. There are two versions of these fabric modules: Fabric1 and Fabric 3. Frames that are received by an FC port with CRC error are dropped and not forwarded further. As frames move from component to component, module to module, including through the fabric modules, errors may occur. Frame CRCs are checked at several places along the switching path. Once a frame error is detected the frame is dropped as soon as possible.

The existing Internal CRC Detection and Isolation feature can detect and take corrective action when these internal CRC errors occur. However, fabric modules can experience other errors that are not true CRC errors. The Fabric Module Error Monitoring feature, introduced in Cisco NX-OS 9.3(1), complements the Internal CRC Detection and Isolation feature, and is designed to detect and take corrective action in the presence of these errors. This feature allows automated monitoring and handling of errors in Fabric 1 and Fabric 3 modules that might cause I/O problems in the fabric.

Fabric Module Error Monitoring is controlled by the **xbarErrorMonitor** CLI command. The command utilizes the MDS scheduler feature to check for the internal errors. It creates a scheduler job named *xbarErrorMonitor_job* with an error checking script and a scheduler schedule named *XbarErrorMonitor_Schedule*. The scheduler periodically executes the script which collects **show hardware internal errors** information for the configurable set of counters on each fabric module. After the configurable sleep time, it collects the **show hardware internal errors** information again and calculates the change of the counter values. If any counter deltas are equal or higher than the configured threshold then the configured action is executed. The **log-only** action will log syslog messages. The module is left in service and continues to switch traffic. The **log-and-out-of-service** action will log the same syslog messages but additionally put the affected module out of service, immediately, stopping the suspect device from affecting further traffic. This action provides real time operational remediation until the module can be later inspected for the root cause. If there is only one fabric module left in service it will not be powered down.

Fabric Module Error Monitoring generates the following type of syslog message detailing the affected module, switching ASIC, error counter, and its value:

%USER-2-SYSTEM_MSG: xbarErrorMonitor: counter threshold exceeded for xbar 1 for counter packets dropped destined to port. (Before: 0, After: 128, Delta 128).

For information about **xbarErrorMonitor** command default values, refer to the Default Values section.

Contact the Cisco Technical Assistance Center (TAC) for diagnostic assistance and possible module replacement if internal CRC errors are detected.

The following error counters can be monitored by Fabric Module Error Monitoring:

| Module | Counter | Description |
|---|---|---|
| Fabric 1 Module | INTERNAL_ERROR_CNT | Errors related to fabric link, input and output buffer full, and timeout events on fabric m |
| | HIGH_XT_DROP_CNT | Packets dropped due to fabric module packet switching timeout. |
| | SAC_XTIMEOUT_INTR_HI | Packet timeouts due to fabric module egress port buffer full. |
| | HIGH_NULL_POE_DROP_CNT | Packets dropped with empty fabric module egress port address. |
| Fabric 3 Module | packets dropped destined to port | Packets dropped due to fabric module egress port buffer full. |
| | packets drop on receive port | Packets dropped on fabric module ingress port. |
| | double bit ecc error | Packets dropped due to double bit ECC error in fabric module port buffers. |
| | null fpoe port | Packets dropped with empty egress port address. |

**Note** These counters can be displayed (if they are non-zero) using the **show hardware internal errors** command.

# Guidelines and Limitations of Fabric Module Error Monitoring

- This feature is supported only on Cisco MDS 9700 series switches.
- Starting from Cisco NX-OS 9.3(1), this feature is enabled automatically.

- Before Cisco NX-OS 9.4(5) xbar error monitoring command has the following behaviour:
  - Any non-default parameters must be specified each time monitoring is enabled. For example:

    ```
    switch# xbarErrorMonitor -si 180 enable
    switch# xbarErrorMonitor -a log-and-out-of-service enable
    ```

  - If the **log-and-out-of-service** option is specified the scheduling interval will be set to the default as the **-si** argument is ignored.

  Starting with Cisco NX-OS 9.4(5) non-default parameters do not need to be specified each time monitoring is enabled. The values displayed with the **show** option are used. Also, the **-si** argument is no longer ignored.
- The *XbarErrorMonitoring_Job* scheduler job and *XbarErrorMonitor_Schedule* scheduler schedule should not be deleted from the configuration or Fabric Module Error Monitoring will cease to function.

# Default Values

Default values are used whenever the parameter is not specified on the **enable** command line.

***Table 7: Fabric Module Error Monitoring default values:***

| Parameter | Default value |
|---|---|
| Action | log-only |

| Parameter | Default value |
|---|---|
| Counters Monitored | NX-OS 9.3(1) - 9.4(4):<br>Fabric 1 Module:<br>• INTERNAL_ERROR_CNT<br>• HIGH_XT_DROP_CNT<br>• SAC_XTIMEOUT_INTR_HI<br>Fabric 3 Module:<br>• packets dropped destined to port<br>• packets drop on receive port<br>• double bit ecc error |
| | NX-OS 9.4(5) and higher:<br>Fabric 1 Module:<br>• INTERNAL_ERROR_CNT<br>• HIGH_XT_DROP_CNT<br>• SAC_XTIMEOUT_INTR_HI<br>• HIGH_NULL_POE_DROP_CNT<br>Fabric 3 Module:<br>• packets dropped destined to port<br>• packets drop on receive port<br>• double bit ecc error<br>• null fpoe port |
| Counter Threshold | NX-OS 9.3(1) - 9.4(4): 50<br>NX-OS 9.4(5) and higher: 10 |
| Scheduler Interval | 120 seconds |
| Sleep Time | 30 seconds |

# Configuring Fabric Module Error Monitoring

### Procedure

**Step 1** switch# **xbarErrorMonitor -h**

Displays command usage and configurable runtime parameters.

**Step 2** switch# **xbarErrorMonitor show**

Displays the status of Fabric Module Error Monitoring.

**Step 3** switch# **xbarErrorMonitor disable**

(Optional) Disables the Fabric Module Error Monitoring feature.

**Step 4** switch# **xbarErrorMonitor enable**

Enables Fabric Module Error Monitoring with default parameters specific to the version of NX-OS.

To modify runtime parameters, specify them as part of this step. Fabric Module Error Monitoring must be disabled before runtime parameters can be modified.

# Alerting for Fabric Module Error Monitoring

### Callhome

In *log-only* mode, threshold breachs will not trigger CallHome alerts.

In *log-and-out-of-service* mode, CallHome will raise an alert when the Fabric Module is taken out of service.

### NDFC

Configure an alarm in NDFC to log alerts when a Fabric Module error occurs.

The alarm severity must match the syslog severity.

The raise and clear regular expressions (regex) must match the whole syslog. Using an identifier variable at the end of the regex will match all text to the end of the syslog.

For clearing, there is no situation where these alarms should be automatically cleared. Each alarm should be manually cleared and investigated. Also, there is no clear syslog message for Fabric Module Error Monitoring events. Use an impossible regex in the alarm's clear regex configuration.

Ensure that the NDFC server IP is configured on the switch as a remote syslog server so the messages reach NDFC.

*Table 8: Example NDFC Alarm Parameters*

| Parameter | Value |
|---|---|
| severity | critical |
| identifier | ID1-ID2 |
| raise regex | USER-2-SYSTEM_MSG xbarErrorMonitor: counter threshold exceeded for xbar $(ID1) for counter $(ID2) |
| clear regex | USER-2-SYSTEM_MSG: place holder regex for $(ID1) and $(ID2) |

For more information about configuring alarms in NDFC, refer to the Event Analytics chapter.

# Configuration Examples

The following example shows how to display the Fabric Module Error Monitoring status and operating values:

```
switch# show xbarErrorMonitor
xbarErrorMonitor 1.2
Status: Enabled
Schedular Interval: 120
Sleep Time: 30
Counter Threshold: 50
Action: log-only
Counters Monitored:
    packets dropped destined to port
    packets drop on receive port
    double bit ecc error
    null fpoe port
```

Thefollowing example shows how to disable Fabric Module Error Monitoring:

```
switch# xbarErrorMonitor disable
xbarErrorMonitor being disabled. Please wait...
xbarErrorMonitor has been disabled.
Please check the status by running 'xbarErrorMonitor show'
It is recommended to execute 'copy running-config startup-config' to save the configuration.
```

The following example shows how to enable Fabric Module Error Monitoring and modify runtime parameters:

```
switch# xbarErrorMonitor --counter-threshold 30 --action
log-and-out-of-service enable
xbarErrorMonitor getting enabled. Please wait...
xbarErrorMonitor has been enabled
Please check the status by running 'xbarErrorMonitor show'
It is recommended to execute 'copy running-config startup-config' to save the configuration.
```