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

First Published: 2022-09-02

Last Modified: 2023-08-18

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

CONTENTS

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 chapters:

Audience

To use this installation guide, you need to be familiar with electronic circuitry and wiring practices, and preferably be an electronic or electromechanical technician.

Document Conventions

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.

Warnings use the following conventions:

Warning 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. Statement 1071.

Related Documentation

The documentation set for the Cisco MDS 9000 Series Switches includes the following documents.

Release Notes

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html

Regulatory Compliance and Safety Information

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/hw/regulatory/compliance/RCSI.html

Compatibility Information

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-device-support-tables-list.html

Installation and Upgrade

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-guides-list.html

Configuration

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-and-configuration-guides-list.html

CLI

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.html

Troubleshooting and Reference

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/tsd-products-support-troubleshoot-and-alerts.html

To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

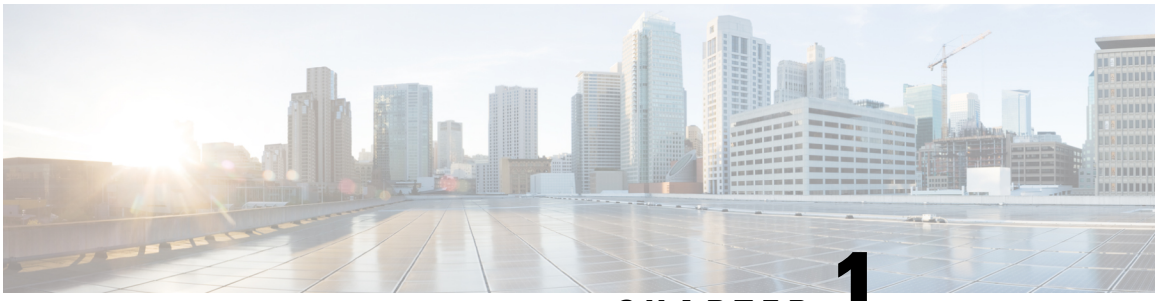
http://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/doclocater.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact 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 Marketplace.
- 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

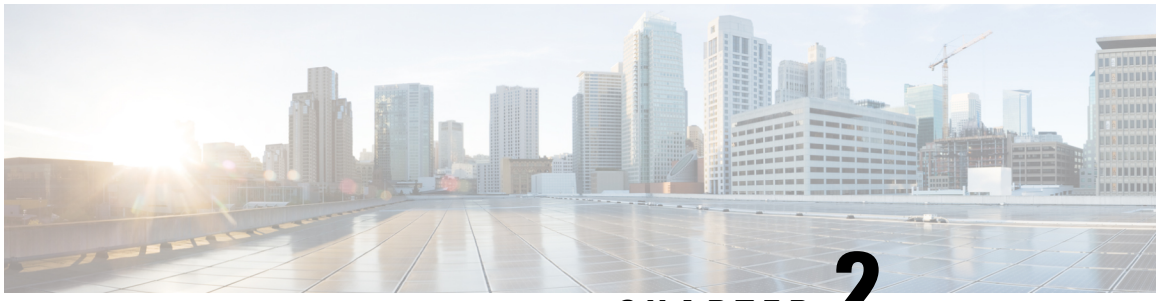
New and Changed Information

This table lists the New and Changed features.

Table 1: New and Changed Features

Feature Name	Description	Release	Where Documented
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. 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. 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 9

Feature Name	Description	Release	Where Documented
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 9
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 9



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

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.

By default, the internal CRC detection and isolation is disabled.

The modules that support this functionality are:

- 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 errors are a separate class of CRC errors when compared to frames that arrive from outside the switch, with CRC errors. In store mode and forward mode, frames with CRC errors are dropped at the ingress port and do not propagate through the system. Internal CRC errors occur when frames are received without errors, but get corrupted when they pass through the switching 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 module to identify an error source.

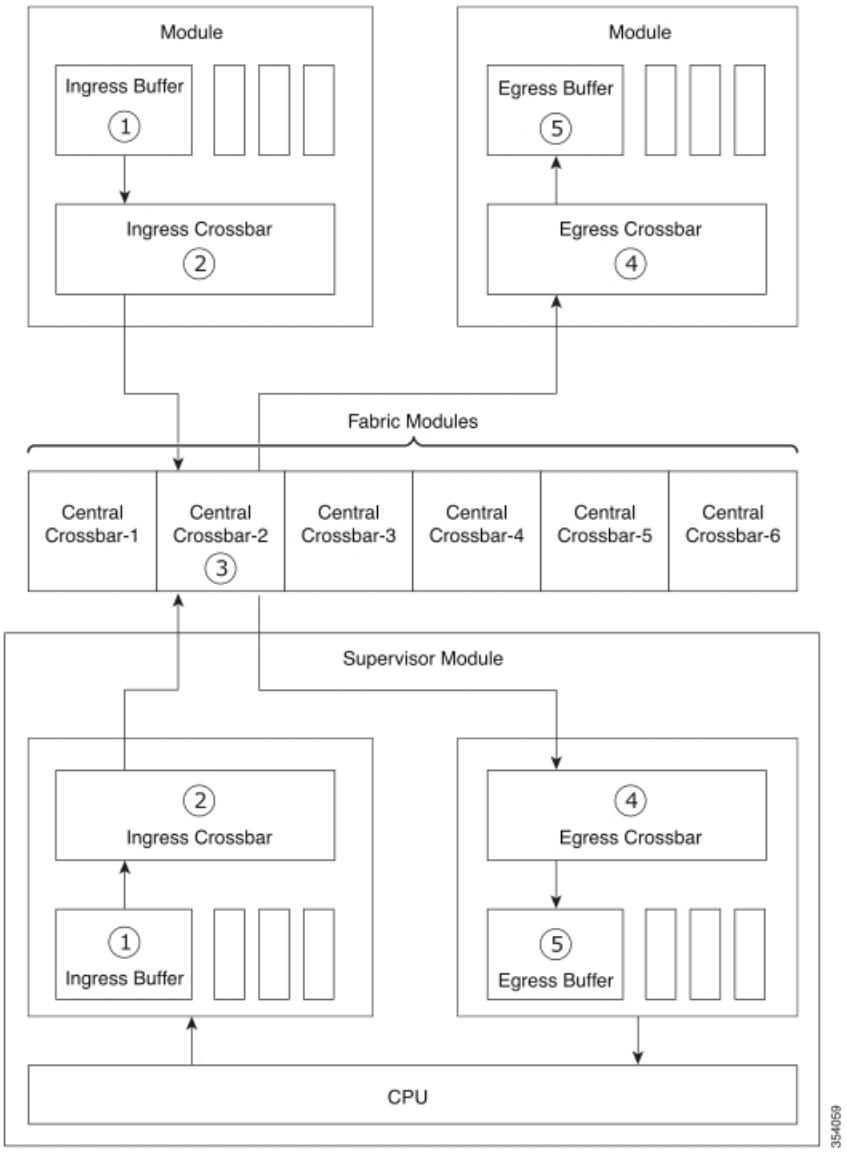
Note The counters are reset at 24 hours from the time the feature, the Internal Cyclic Redundancy Check (CRC) detection and isolation was first configured.

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 host fabric module 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

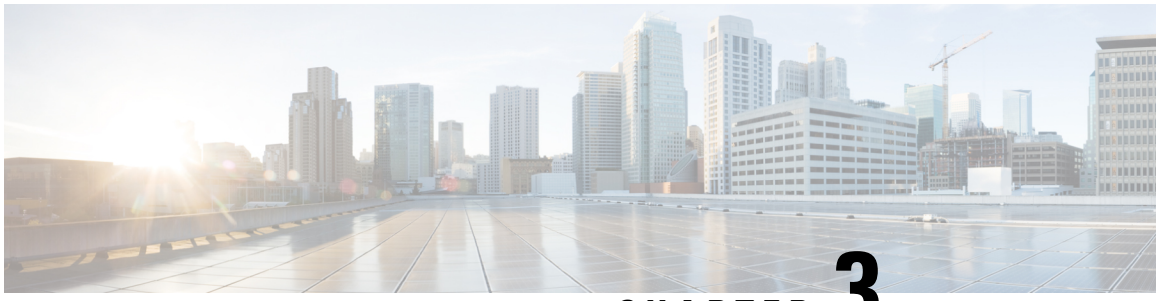
The actions taken on a supervisor when the threshold is exceeded during the following stages of internal CRC detection and isolation:

1. **Stage 1**—Ingress Buffer of a Module
2. **Stage 2**—Ingress Crossbar of a Module
3. **Stage 3**—Central Crossbar of a Chassis
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 a single fabric module is present and Stage 2 error occurs, the line card connected to the fabric module is powered down; as a result the switch is brought down. This mechanism helps in isolating the faulty spine port or link as the line card connected to the spine which experienced the error is brought down.

For information on configuring the Internal CRC Detection and Isolation feature, see Configuring Internal CRC Detection and Isolation, on page 13.



CHAPTER 3

Configuring High Availability

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

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://tools.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. 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. 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. The following command was modified: **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:

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:

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 15 and Table 6: Internal States , on page 16 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.
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. **Note** 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.

State	Description
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.
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.