Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.2(8i)

First Published: November 24, 2016

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 25.

Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.html

Contents

This document includes the following:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

> **Note** The Cisco MDS NX-OS Release 5.2(8i) is supported only on the Cisco MDS 9124 Multilayer Fabric Switch.

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides industry-leading availability, scalability, security, and management, allowing you to deploy high-performance storage-area networks with the lowest total cost of ownership. Layering a rich set of intelligent features onto a high-performance, protocol-agnostic switch fabric, the Cisco MDS 9000 Family addresses the stringent requirements of large data center storage environments: uncompromising high availability, security, scalability, ease of management, and seamless integration of new technologies.

Cisco MDS 9000 NX-OS software powers the award-winning Cisco MDS 9000 Series Multilayer Switches. It is designed to create a strategic SAN platform with superior reliability, performance, scalability, and features. Formerly known as Cisco SAN-OS, Cisco MDS 9000 NX-OS software is fully interoperable with earlier Cisco SAN-OS versions and enhances hardware platform and module support.

Components Supported

For the latest information about supported Small Form-Factor Pluggable (SFP), Enhanced Small Form-Factor Pluggable (SFP+), and X2 devices, see the *Cisco MDS 9000 Family Pluggable Transceivers* data sheet.

Table 1 lists the NX-OS software part numbers and hardware components supported by the Cisco MDS 9000 Family.

Table 1   Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M91S2K9-5.2.8i	MDS 9100, NX-OS software	MDS 9124 Switch
Chassis	DS-C9124-K9	Cisco MDS 9124 24-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 24 4-Gbps Fibre Channel ports)	MDS 9124 Switch
MDS Fibre Channel Blade Switches	DS-IBM-FC-K9	IBM Cisco MDS Fibre Channel blade switch	9100 Series
	DS-HP-FC-K9	HP Cisco MDS 9124e Fibre Channel blade switch for HP C Class Blade Switch	9100 Series
	DS-HP-8GFC-K9	8-Gbps FC Switch for HP Blade System	9100 Series
Power Supplies	DS-C24-300AC	300W AC power supply	MDS 9124 Switch

MDS 9000 Chassis and Module Support

> **Note** The Cisco MDS NX-OS Release 5.2(8i) is supported only on the Cisco MDS 9124 Multilayer Fabric Switch.

Table 2 lists the MDS hardware chassis supported by Cisco MDS NX-OS 5.x.

Table 2   Cisco MDS NX-OS 5.x Chassis Support Matrix

Switch	NX-OS 5.x Support
MDS 9124	Yes[a]

a. This switch supports Cisco MDS NX-OS Release 5.2(2) and later releases, but does not support Release 5.2(1).

Table 3 lists the MDS hardware modules supported by Cisco MDS NX-OS 5.x. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 4.x, see Table 4. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 3.x, see Table 5.

Table 3   Module Support Matrix for Cisco MDS NX-OS 5.x

Module	Description	MDS 9500 Series		MDS 9222i	
		NX-OS 5.2(x)	NX-OS 5.0(x)	NX-OS 5.2(x)	NX-OS 5.0(x)
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	Yes	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes	Yes	N/A	N/A
DS-13SLT-FAB3	MDS 9513 Fabric Module 3	Yes	No	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	Yes	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	Yes	N/A	N/A
DS-X9708-K9	8-port 10-Gbps FCoE Module	Yes[a,b]	No	No	No
DS-X9232-256K9	32-port 8-Gbps Advanced Fibre Channel Switching Module	Yes[a]	No	No	No
DS-X9248-256K9	48-port 8-Gbps Advanced Fibre Channel Switching Module	Yes[a]	No	No	No
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[a]	Yes[c]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[a]	Yes[c]	No	No
DS-X9248-48K9	4/44-port Host Optimized 8-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes

Table 3   ***Module Support Matrix for Cisco MDS NX-OS 5.x (Continued)***

Module	Description	MDS 9500 Series		MDS 9222i	
		NX-OS 5.2(x)	NX-OS 5.0(x)	NX-OS 5.2(x)	NX-OS 5.0(x)
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes

a.Requires DS-13SLT-FAB3 or DS-13SLT-FAB2 in the MDS 9513.

b.Requires the Supervisor-2A module.

c.Requires DS-13SLT-FAB2 in the MDS 9513.

Table 4   ***Module Support Matrix for Cisco MDS NX-OS 4.x***

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes[a]	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	No	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[b]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[b]	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	Yes	Yes	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	No	No	No
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	No	No	No

a.In software releases earlier than Cisco NX-OS Release 4.2(7a), the Supervisor-2A module appears as unsupported hardware in Device Manager, but the Supervisor-2A module does work with Cisco NX-OS release 4.x software.

b.Requires DS-13SLT-FAB2 in the MDS 9513.

Table 5 lists the MDS hardware modules supported by Cisco MDS SAN-OS 3.x.

Table 5   Module Support Matrix for Cisco MDS SAN-OS 3.x

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes[a]	N/A	N/A	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A	N/A	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)[b]	Yes	Yes	Yes	Yes	No
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes	Yes	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	Yes	No	Yes	Yes	Yes
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	Yes	Yes	Yes	Yes	Yes

a.In software releases earlier than Cisco NX-OS Release 3.3(5a), the Supervisor-2A module appears as unsupported hardware in Device Manager, but the Supervisor-2A module does work with Cisco NX-OS release 3.x software.

b.Cisco SAN-OS Release 3.2(1) and later support the 18/4-Port Multiservice Module (MSM-18/4).

Software Download Process

Use the software download procedure to upgrade to a later version, or downgrade to an earlier version, of an operating system. This section describes the software download process for the Cisco MDS NX-OS software and includes the following topics:

Determining the Software Version

To determine the version of Cisco MDS NX-OS or SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log in to the switch and enter the **show version** EXEC command.

To determine the version of Cisco MDS NX-OS or SAN-OS software currently running on a Cisco MDS 9000 Family switch using Cisco DCNM for SAN, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.

Determining Software Version Compatibility

Table 6 lists the software versions that are compatible in a mixed SAN environment, the minimum software versions that are supported, and the versions that have been tested. We recommend that you use the latest software release supported by your vendor for all Cisco MDS 9000 Family products.

Table 6   Software Release Compatibility

Cisco NX-OS Software	Minimum NX-OS or SAN-OS Release	Tested NX-OS and SAN-OS Releases
NX-OS Release 5.2(8i)	NX-OS Release 5.2(1) or later	NX-OS Release 5.2(1) or later
	NX-OS Release 5.0(1a) or later	NX-OS Release 5.0(1a) and later
	NX-OS Release 4.2(3) or later	NX-OS Release 4.2(3) and later
	SAN-OS Release 3.3(5) or later	SAN-OS Release 3.3(5) and later

Downloading Software

The Cisco MDS NX-OS software is designed for mission-critical high availability environments. To realize the benefits from nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

To download the latest Cisco MDS NX-OS software, access the Software Center at this URL:

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

See the following sections in this release note for details on how you can nondisruptively upgrade your Cisco MDS 9000 switch. Issuing the **install all** command from the CLI, or using Cisco DCNM for SAN to perform the downgrade, enables the compatibility check. The check indicates if the upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch and the reason.

```
Compatibility check is done:
Module  bootable         Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes      disruptive       rolling  Hitless upgrade is not supported
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset
```

The **show incompatibility system bootflash**:*system image filename* command determines which additional features need to be disabled.

Note If you would like to request a copy of the source code under the terms of either GPL or LGPL, send an e-mail to mds-software-disclosure@cisco.com.

Selecting the Correct Software Image for an MDS 9100 Series Switch

The system and kickstart image that you use for an MDS 9100 Series switch depends on which switch you use, as shown in Table 7.

Table 7   Software Images for MDS 9100 Series Switches

Cisco MDS 9100 Series Switch Type	Naming Convention
MDS 9134, MDS 9124, Cisco MDS 4-Gbps Fabric Switch for HP c-Class BladeSystem, Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter	Filename begins with m9100-s2ek9

NPE Software Images

No payload encryption (NPE) images are available with some releases of Cisco MDS NX-OS Release 5.2(x) software. The NPE images are intended for countries who have import restrictions on products that encrypt payload data.

To differentiate an NPE image from the standard software image, the letters npe are included in the image name as follows:

- m9100-s2ek9-kickstart-mz-npe.5.2.8i.bin

- m9100-s2ek9-mz-npe.5.2.8i.bin

When downloading software, ensure that you select the correct software images for you Cisco MDS 9000 Series switch. Nondisruptive software upgrades or downgrades between NPE images and non-NPE images are not supported.

Upgrading Your Cisco MDS NX-OS Software Image

This section lists the guidelines recommended for upgrading your Cisco MDS NX-OS software image and includes the following topics:

✎

Note Before you begin the upgrade process, review the list of chassis and modules that Cisco MDS NX-OS Release 5.2(8i) supports. See the "MDS 9000 Chassis and Module Support" section on page 2.

For detailed instructions for performing a software upgrade using Cisco DCNM, see the *Cisco DCNM Release Notes, Release 5.2*, which is available from the following website:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/products-release-notes-list.html

Upgrading Guidelines Specific to NX-OS Release 5.2(8i)

Before upgrading your Cisco NX-OS software, you must determine if the following issue has occurred in your switch:

```
%FLOGI-1-MSG_FLOGI_REJECT_FCID_ERROR after upgrade/switchover
```

An ISSU or ISSD involves a supervisor switchover, so it is very important that you determine if this issue is present before a supervisor switchover occurs. If this issue is detected before the supervisor switchover, the affected interfaces can be restored easily by entering the **shutdown** and **no shutdown** command sequence.

The following example shows how to determine if the issue has occurred before a supervisor switchover:

```
switch# show flogi internal info | i key|Interface | i key p 1
Interface fc4/32: mode[F] [119f000] Mode: F State: UP Vsan: 237
  Vsan no:237 Max flogi key:0x1002a(65578) num_fl[0x1]<<<Max flogi key greater than 65535
--
Interface fc6/32: mode[F] [129f000] Mode: F State: UP Vsan: 237
  Vsan no: 237 Max flogi key: 0x1(1) num_fl[0x1]
--
```

Look for the value for a Max flogi key that is greater than 65535.

In the example, the fc4/32 interface has encountered this issue, but the fc6/32 interface is normal.

If you see that an interface has a Max flogi key greater than 65535 before a system switchover, ISSU, or ISSD, you must disable the interface and then reenable it by using the **shutdown** command followed by the **no shutdown** command. This process disrupts the devices on the interface that is being shut down. After the devices relogin, the Max flogi key is reset to 1 and you can avoid this issue.

If an install and/or ISSU, or supervisor switchover has occurred, compare the number of devices fabric login (FLOGI) with the number of devices in the Fibre Channel Name Server (FCNS) local database. Enter the **show flogi database** and the **show fcns database local** commands and use the CLI outputs for comparison. If the FLOGI database has fewer entries than the FCNS local database, the issue has occurred.

Also, if the following error message appears after an install, ISSU, or supervisor switchover, the issue might bug may have been encountered:

```
 %FLOGI-1-MSG_FLOGI_REJECT_FCID_ERROR: %$VSAN xxx%$ [VSAN xxx, Interface fc4/19: mode[F]]
FLOGI rejected - FCID allocation failed with error 0x401b0000.
```

If you observe either of the above situations, open a case with the Cisco TAC.

Note If the Max flogi key value is a large number and is incrementing, it indicates that a device is repeatedly logging in. This situation might be a separate problem that needs further investigation. For assistance, contact the Cisco TAC.

In addition, follow these guidelines when upgrading to Cisco MDS NX-OS Release 5.2(8i):

- Follow the upgrade path to NX-OS Release 5.2(8i) that is specified in Table 8.

- Upgrade to NX-OS Release 5.2(x) before you install any Advanced 8-Gbps module in an MDS 9500 Series switch. NX-OS Release 5.2(x) is needed for the switch to recognize the new hardware.

- We recommend that you delete any SPAN configuration, Fibre Channel tunnel, or tunnel-ID map configuration from your switch before you start the upgrade to NX-OS Release 5.2(8i). You can save the SPAN destination and SPAN target configuration and then reconfigure the SPAN session following the upgrade. All SPAN destination and SPAN target ports are reinitialized after the upgrade. To gather information about SPAN sessions and delete them, use the following commands in this order:

    - **show incompatibility systems bootflash:***image_name* to display any incompatible configurations

    - **show span session** to check the current configuration for a SPAN session

    - **no span session** *session-number* to delete a SPAN session

    - **show running-config | include fc-tunnel** to check the current Fibre Channel tunnel configuration

    - **no interface fc-tunne**l *y* to delete a Fibre Channel tunnel on the switch that is the source for the Fibre Channel tunnel

    - **show interface brief | include SD** to check the current configuration for a SPAN destination port configuration

    - **show interface brief | include ST** to check the current configuration for a SPAN target port configuration

    - **no fc-tunnel tunnel-map** *z* **interface** *x/y* to remove an Fibre Channel tunnel map

    - **no switchport mode sd** to negate the SPAN destination port mode for the SPAN destination port

    - **no switchport mode st** to negate the SPAN target port mode for the SPAN target port

- If you are using IVR non-NAT mode, migrate to IVR-NAT mode before you upgrade to NX-OS Release 5.2(8i). IVR non-NAT mode is deprecated in NX-OS Release 5.2(1).

    Note In dual SAN fabrics, IVR traffic can use one fabric while the other fabric is migrating. Only IVR traffic is disrupted during the migration. Regular traffic within the VSAN is not disrupted during the migration.

    To migrate to IVR-NAT mode, follow these steps:

    1. Stop or divert all applications on servers that depend on IVR.

- – If CFS distribution is not enabled for IVR, then perform steps 2 through 4 on all switches where IVR is enabled.

- – If CFS distribution is enabled for IVR, then enter the **ivr commit** command following step 2, step 3, and step 4 to distribute the changes to other switches.

2. Deactivate the IVR zone set by entering the **no ivr zoneset activate** command.

3. Enable IVR NAT by entering the **ivr nat** command.

4. Activate the IVR zone set by entering the **ivr zoneset activate** command.

5. Start or reestablish all applications that were stopped in step 1.

The network can now run in IVR-NAT mode.

General Upgrading Guidelines

Follow these general guidelines before performing a software upgrade:

- Review the nondisruptive upgrade path to Release 5.2(8i) in Table 8.

- Install and configure dual supervisor modules before the upgrade.

- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.

- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:

  - – **Fibre Channel Ports**: Fibre Channel ports can be nondisruptively upgraded without affecting traffic on the ports. See Table 8 for the nondisruptive upgrade path for all NX-OS and SAN-OS releases.

Note In addition to these guidelines, you may want to review the information in the "Limitations and Restrictions" section prior to a software upgrade to determine if a feature may possibly behave differently following the upgrade.

Upgrade Paths

Open Systems Upgrade Paths

Use Table 8 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 5.2(8i). Find the image release number you are currently using in the "Current Release" column of the table and follow the steps in the order specified to perform the upgrade.

Note The software upgrade information in Table 8 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and intelligent services traffic.

Table 8   Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 5.2(8i)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
All 5.2(x) releases	Upgrade directly to Cisco NX-OS Release 5.2(8i).

Table 8 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 5.2(8i) (Continued)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
All 5.0(x) releases	Upgrade directly to Cisco NX-OS Release 5.2(8i).
All 4.2(x) releases and 4.1(x) releases	1. Upgrade to Cisco NX-OS Release 5.0(8a). 2. Upgrade to Cisco NX-OS Release 5.2(8i).
SAN-OS:	
Release 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	1. Upgrade to Cisco NX-OS Release 4.2(9). 2. Upgrade to Cisco NX-OS Release 5.0(8a). 3. Upgrade to Cisco NX-OS Release 5.2(8i).
Release 3.3(1c), all 3.2(x), 3.1(x), and 3.0(x) releases)	1. Upgrade to Cisco SAN-OS Release 3.3(5b). 2. Upgrade to Cisco NX-OS Release 4.2(9). 3. Upgrade to Cisco NX-OS Release 5.0(x). 4. Upgrade to Cisco NX-OS Release 5.2(8i).
Release 2.1(3), 2.1(2e), 2.1(2d), and 2.1(2b)	1. Upgrade to Cisco SAN-OS Release 3.3(1c). 2. Upgrade to Cisco SAN-OS Release 3.3(5b). 3. Upgrade to Cisco NX-OS Release 4.2(9). 4. Upgrade to Cisco NX-OS Release 5.0(8a). 5. Upgrade to Cisco NX-OS Release 5.2(8i).
Release 2.1(2), 2.1(1b), 2.1(1a), and 2.0(x)	1. Upgrade to Cisco SAN-OS Release 2.1(2b), 2.1(2d), 2.1(2e), or 2.1(3) 2. Upgrade to Cisco SAN-OS Release 3.3(1c). 3. Upgrade to Cisco SAN-OS Release 3.3(5b). 4. Upgrade to Cisco NX-OS Release 4.2(9). 5. Upgrade to Cisco NX-OS Release 5.0(8a). 6. Upgrade to Cisco NX-OS Release 5.2(8i).
Release 1.x	1. Upgrade to Cisco SAN-OS Release 1.3(4a). 2. Upgrade to Cisco SAN-OS Release 2.1(2b). 3. Upgrade to Cisco SAN-OS Release 3.3(1c). 4. Upgrade to Cisco SAN-OS Release 3.3(5b). 5. Upgrade to Cisco NX-OS Release 4.1(x) or 4.2(x). 6. Upgrade to Cisco NX-OS Release 5.0(8a). 7. Upgrade to Cisco NX-OS Release 5.2(8i).

Downgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for downgrading your Cisco MDS SAN-OS software image and includes the following topics:

- Downgrading Guidelines Specific to NX-OS Release 5.2(8i), page 12
- General Downgrading Guidelines, page 12

Downgrading Guidelines Specific to NX-OS Release 5.2(8i)

The following guidelines apply to a downgrade from Cisco MDS NX-OS Release 5.2(8i):

- Cisco NX-OS Release 5.2(6) and later releases support IDLE as a fill word for the switchport fill-pattern command. Releases earlier than Release 5.2(6) supported only the ARBFF fill word. As a result, when you downgrade from Cisco NX-OS Release 5.2(6) or a later release to an earlier release that does not support the IDLE fill word, the following syntax error occurs:

  ```
  Syntax error while parsing 'switchport fill-pattern IDLE speed 8000'
  ```

  The syntax error message is harmless and can be ignored.

- If smart zoning is enabled on your system and you want to downgrade nondisruptively to a version lower than NX-OS Release 5.2(6), you must disable smart zoning on all VSANs.

- We recommend that you delete any SPAN configuration, Fibre Channel tunnel, or tunnel-ID map configuration from your switch before you downgrade from NX-OS Release 5.2(8i) to a lower version. If any SPAN session, SPAN destination, SPAN target, or Fibre Channel tunnel interface is configured, the installer should detect it and prompt you to delete these configurations.

  To gather information about SPAN sessions and delete them, use the following commands in this order:

  - **show incompatibility systems bootflash:***image_name* to display any incompatible configurations
  - **show span session** to check the current configuration for a SPAN session
  - **no span session** *session-number* to delete a SPAN session
  - **show running-config | include fc-tunnel** to check the current Fibre Channel tunnel configuration
  - **no interface fc-tunne**l *y* to delete a Fibre Channel tunnel on the switch that is the source for the Fibre Channel tunnel
  - **show interface brief | include SD** to check the current configuration for a SPAN destination port configuration
  - **show interface brief | include ST** to check the current configuration for a SPAN target port configuration
  - **no fc-tunnel tunnel-map** *z* **interface** *x/y* to remove an Fibre Channel tunnel map
  - **no switchport mode sd** to negate the SPAN destination port mode for the SPAN destination port
  - **no switchport mode st** to negate the SPAN target port mode for the SPAN target port

General Downgrading Guidelines

Follow these general guidelines before you perform a software downgrade:

- Disable all features not supported by the downgrade release. Use the **show incompatibility system** *downgrade-image* command to determine what you need to disable.

- Use the **show install all impact** *downgrade-image* command to determine if your downgrade will be nondisruptive.

- Be aware that some features impact whether a downgrade is disruptive or nondisruptive:

  - **Fibre Channel Ports**: Fibre Channel ports can be nondisruptively downgraded without affecting traffic on the ports.

New Features in Cisco MDS NX-OS Release 5.2

This section lists the new software and hardware features in Cisco MDS NX-OS Release 5.2. It includes the following topics:

Product information about Cisco MDS 9000 NX-OS software is available at this link:

http://www.cisco.com/en/US/products/ps5989/index.html

New Features in Cisco MDS NX-OS Release 5.2(8i)

Cisco MDS NX-OS Release 5.2(8i) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8h)

Cisco MDS NX-OS Release 5.2(8h) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8g)

Cisco MDS NX-OS Release 5.2(8g) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8f)

Cisco MDS NX-OS Release 5.2(8f) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8e)

Cisco MDS NX-OS Release 5.2(8e) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8d)

This section briefly describes the new software features introduced in Cisco NX-OS Release 5.2(8d).

- Restriction of the number of NPIV logins to not exceed the configuration limits in for Cisco MDS 9500 Series switches

Command-line interface (CLI) command changes, including the following:

- **switchport**: added the **max-npiv-limit** and **trunk-max-npiv-limit** keywords.

New Features in Cisco MDS NX-OS Release 5.2(8c)

Cisco MDS NX-OS Release 5.2(8c) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8b)

Cisco MDS NX-OS Release 5.2(8b) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8a)

Cisco MDS NX-OS Release 5.2(8a) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(8)

Cisco MDS NX-OS Release 5.2(8) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(6b)

Cisco MDS NX-OS Release 5.2(6b) is a maintenance release that includes bug fixes. It does not include new features.

New Features in Cisco MDS NX-OS Release 5.2(6a)

Cisco MDS NX-OS Release 5.2(6a) is a maintenance release that includes bug fixes and a scalability improvement for the following feature:

- Cisco I/O Accelerator

    Starting with Cisco MDS NX-OS Release 5.2(6a), the number of supported I/O Accelerator (IOA) flows has increased to 1248.

New Features in Cisco MDS NX-OS Release 5.2(6)

Cisco MDS NX-OS Release 5.2(6) includes the new features described in the following sections:

- Smart Zoning, page 15

Smart Zoning

Cisco Smart Zoning simplifies the process of zoning to reduce the burden on administrators while simultaneously provisioning zone-related hardware resources on Cisco Fibre Channel switching modules more efficiently.

For more information on configuring and deploying Smart Zoning, see the *Cisco MDS 9000 Fabric Configuration Guide.*

New Features in Cisco MDS NX-OS Release 5.2(2d)

Cisco MDS NX-OS Release 5.2(2d) is a maintenance release that includes bug fixes. It does not include any new features.

New Features in Cisco MDS NX-OS Release 5.2(2a)

Cisco MDS NX-OS Release 5.2(2a) is a maintenance release that includes bug fixes and the following feature enhancement:

- Port Monitor

    Port monitoring has been enhanced with several ASIC counters that monitor and report internal packet drops.

    Additional information about this feature enhancement is available in the *Cisco MDS 9000 Series Interfaces Configuration Guide.*

New Features in Cisco MDS NX-OS Release 5.2(2)

Cisco MDS NX-OS Release 5.2(2) is a FICON-certified version of Cisco MDS NX-OS Release 5.2(1), that also includes new features and bug fixes. In addition to these features, Cisco MDS NX-OS Release 5.2(2) supports all the new software features and new hardware that were introduced in Cisco MDS NX-OS Release 5.2(1).

Cisco MDS NX-OS Release 5.2(2) supports the following software features:

- FICON Certification

  Cisco MDS NX-OS Release 5.2(2) is a FICON-certified release that supports these features:

  - Nondisruptive software upgrades to and downgrades from Cisco NX-OS Release 4.2(7b), which is the previous FICON-certified release.

  - FICON FCIP on the Cisco MDS 9000 SSN-16 module, including FICON Tape Acceleration and XRC Acceleration.

  - FICON Tape Acceleration for ESCON through Optica PRIZM.

  - FICON support on the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module, the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module, and the Cisco MDS 9513 Switching Fabric 3 module (DS-13SLT-FAB3).

- Availability of Cisco MDS NX-OS Release 5.2 on Cisco MDS 9100 Series Fabric Switches

  Cisco MDS NX-OS Release 5.2(2) supports the following switches (which are not supported by Cisco MDS NX-OS Release 5.2(1)):

  - Cisco MDS 9134 Fabric Switch

  - Cisco MDS 9124 Fabric Switch

  - Cisco MDS 4-Gbps Fabric Switch for HP c-Class BladeSystem

  - Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter

- Port Group Monitoring

  Port group monitoring and SNMP are available on the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module and the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module.

- Availability of IVR on the Cisco MDS 9148 Switch

  Cisco MDS NX-OS Release 5.2(2) supports Inter-VSAN Routing (IVR) on the Cisco MS 9148 multilayer fabric switch.

- IOA with NPV

  Cisco MDS NX-OS Release 5.2(2) supports configuring IOA with NPV.

New Features in Cisco MDS NX-OS Release 5.2(1)

Cisco MDS NX-OS Release 5.2(1) supports the following software features:

- Software support for the MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module

  The MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module is a multihop-capable FCoE module for the core data center. This full line-rate FCoE module for the MDS 9500 Series Director switches allows you to extend FCoE benefits beyond the access layer into the data center core. FCoE supports I/O consolidation by preserving all Fibre Channel constructs, and maintaining the same latency, security, and traffic management attributes of Fibre Channel. In addition, FCoE extends Fibre Channel SAN connectivity to Cisco Nexus 7000 switches that are FCoE capable.

- Software support for Cisco MDS 9000 Family 8-Gbps Advanced Fibre Channel Switching Modules

  Cisco NX-OS Release 5.2(1) includes software support for the 32-port and the 48-port 8-Gbps Advanced Fibre Channel switching modules that can be used in the MDS 9500 Series Directors. The MDS 9513 Multilayer Director can be upgraded with the new Generation 4 Fabric-3 module to

increase bandwidth to 256 Gbps per slot. In addition, the 8-Gbps Advance Fibre Channel switching module support speeds of 10 Gbps on the MDS 9513 with the Fabric-3 module installed. The upgrade from the Fabric-2 module to the Fabric-3 module is nondisruptive.

Cisco MDS 9000 8-Gbps Advanced Fibre Channel switching modules support Cisco FlexSpeed technology that enables ports to be configured as either 1-, 2-, 4-, or 8-Gbps, or 10-Gbps Fibre Channel interfaces.

Cisco MDS 9000 8-Gbps Advanced Fibre Channel switching modules support Arbitrated Local Switching to locally switch traffic at line rate 8-Gbps in a fair manner across all ports on the module through central arbitration.

- Storage Media Encryption for Disk

  The Storage Media Encryption (SME) solution, which currently protects data at rest on heterogeneous tape drives and virtual tape libraries (VTLs), has been enhanced to encrypt data on disk arrays in a SAN environment using secure IEEE-standard Advanced Encryption Standard (AES) algorithms.

  SME Disk requires the Storage Media Encryption Package license.

  See the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide* for more information on configuring and deploying SME Disk.

- Cisco Data Center Network Manager for SAN

  Cisco Fabric Manager and Cisco Data Center Network Manager have merged into a unified product that can now manage and monitor both SAN and LAN environments. As a part of this merger, Cisco Fabric Manager has been rebranded as Cisco DCNM for SAN.

  As a part of NX-OS Release 5.2(1), Cisco DCNM for SAN introduces server-based licenses that allow you to purchase a pool of Cisco DCNM for SAN licenses instead of a switch-based Fabric Manager Server (FMS) license. The installed base of existing FMS licenses are grandfathered into Cisco DCNM for SAN, which means that you do not have to purchase a new license to use Cisco DCNM for SAN if you have an existing FMS license.

  There are many new features in Cisco DCNM for SAN, including:

  - Summary and host dashboards
  - VMware topology and performance
  - Performance forecasting charts
  - External SMI-S 1.4 agent
  - FCoE provisioning and management

  Detailed information about Cisco DCNM features is available in the *Cisco DCNM Release Notes, Release 5.2,* and in the feature configuration guides for Cisco DCNM for SAN.

For additional information about Cisco MDS NX-OS Release 5.2(1), see the *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.2(1).*

New Hardware Supported in Cisco MDS NX-OS Release 5.2(1)

Cisco MDS NX-OS Release 5.2(1) supports the following new Generation 4 hardware devices:

- Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module (DS-X9708-K9)
- Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module (DS-X9232-256K9)
- Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module (DS-X9248-256K9)

- Cisco MDS 9513 Switching Fabric 3 module (DS-13SLT-FAB3)

See the *Cisco MDS 9500 Series Hardware Installation Guide* for descriptions of, and specifications for the new Generation 4 modules. This guide also provides instructions for migrating to the new Fabric 3 module and guidelines for installing the new 8-Gbps Advanced Fibre Channel switching modules.

Licensed Cisco NX-OS Software Packages

Most Cisco MDS 9000 family software features are included in the standard package. However, some features are logically grouped into add-on packages that must be licensed separately, such as the Cisco MDS 9000 Enterprise package, SAN Extension over IP package, Mainframe package, Storage Services Enabler (SSE) package, Storage Media Encryption package, and Data Mobility Manager package. On-demand ports activation licenses are also available for the Cisco MDS Blade Switch Series and 4-Gbps Cisco MDS 9100 Series Multilayer Fabric switches.

Note A license is not required to use the Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module (DS-X9708-K9).

Enterprise Package

The standard software package that is bundled at no charge with the Cisco MDS 9000 Family switches includes the base set of features that Cisco believes are required by most customers for building a SAN. The Cisco MDS 9000 family also has a set of advanced features that are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Enterprise package. Refer to the Cisco MDS 9000 Enterprise package fact sheet for more information. Mainframe Package

The Cisco MDS 9000 Mainframe package uses the FICON protocol and allows control unit port management for in-band management from IBM S/390 and z/900 processors. FICON VSAN support is provided to help ensure true hardware-based separation of FICON and open systems. Switch cascading, fabric binding, and intermixing are also included in this package. Refer to the Cisco MDS 9000 Mainframe package fact sheet for more information.

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco NX-OS Software features while initially purchasing only a small number of activated ports on 8-Gbps or 4-Gbps Cisco MDS 9100 Series Multilayer Fabric switches. As needed, customers can expand switch connectivity by licensing additional ports.

Deprecated Features

Cisco MDS NX-OS Release 5.2 no longer supports the features listed in the following sections:

- Zoning Features, page 19
- SNIA Common Information Model, page 19

Zoning Features

LUN zoning, read-only zones, and broadcast zones are no longer supported. These features affect the following hardware:

- Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module
- Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module
- Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module

You cannot bring up these modules if these features are already configured. You should completely remove all configurations that include these features before you attempt to bring up these modules. In addition, you cannot configure these features after you bring up these modules.

SNIA Common Information Model

SNIA Common Information Model (CIM or cimserver) commands are no longer supported. CIM is supported in Cisco DCNM-SAN Release 5.2. The SMI-S agent that is installed on the Cisco DCNM-SAN server allows external application to access fabric and switch profiles as specified in SNIA CIM. For additional information, see the *Cisco DCNM Release Notes, Release 5.2.*

Limitations and Restrictions

This section lists the limitations and restrictions. The following limitations are described:

- Cisco DCNM compatibility with Cisco MDS NX-OS Release 5.2(8i), page 19
- IPv6, page 20
- User Roles, page 20
- Schedule Job Configurations, page 20
- Maximum Number of Zones Supported in Interop Mode 4, page 20
- Java Web Start, page 20
- Using a RSA Version 1 Key for SSH Following an Upgrade, page 21
- CFS Cannot Distribute All Call Home Information, page 21
- Availability of F Port Trunking and F Port Channels, page 22
- Reserved VSAN Range and Isolated VSAN Range Guidelines, page 22
- Applying Zone Configurations to VSAN 1, page 23
- RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules, page 23
- Saving Copies of the Running Kickstart and System Images, page 23
- Configuring Buffer Credits on a Generation 2 or Generation 3 Module, page 23

Cisco DCNM compatibility with Cisco MDS NX-OS Release 5.2(8i)

Cisco Prime DCNM support for Cisco MDS NX-OS Release 5.2(8i) starts from Cisco Prime DCNM Release 7.2(1). Using releases earlier than Cisco Prime DCNM Release 7.2(1) with Cisco MDS NX-OS Release 5.2(8i) causes authentication failure. See CSCun41202 for more information.

IPv6

The management port on Cisco MDS switches supports one user-configured IPv6 address, but does not support auto-configuration of an IPv6 address.

User Roles

In SAN-OS Release 3.3(x) and earlier, when a user belongs to a role which has a VSAN policy set to Deny and the role allows access to a specific set of VSANs (for example, 1 through 10), the user is restricted from performing the **configuration**, **clear**, **execute**, and **debug** commands which had a VSAN parameter outside this specified set. Beginning with NX-OS Release 4.1(1b), these users are still prevented from performing **configuration**, **clear**, **execute**, and **debug** commands as before, however, they are allowed to perform **show** commands for all VSANs. The ability to execute the **show** command addresses the following:

- In a network environment, users often need to view information in other VSANs even though they do not have permission to modify configurations in those VSANs.

- This behavior makes Cisco MDS 9000 Series switches consistent with other Cisco products, such as Cisco Nexus 7000 Series switches, that exhibit the same behavior for those roles (when they apply to the VLAN policy).

Schedule Job Configurations

As of MDS NX-OS Release 4.1(1b) and later, the scheduler job configurations need to be entered in a single line with a semicolon(;) as the delimiter.

Job configuration files created with SAN-OS Release 3.3(1c) and earlier, are not supported. However, you can edit the job configuration file and add the delimiter to support Cisco NX-OS Release 4.1(3a).

Maximum Number of Zones Supported in Interop Mode 4

In interop mode 4, the maximum number of zones that is supported in an active zone set is 2047, due to limitations in the connected vendor switch.

When IVR is used in interop mode 4, the maximum number of zones supported, including IVR zones, in the active zone set is 2047.

Java Web Start

When using Java Web Start, we recommend that you do not use an HTML cache or proxy server. You can use the Java Web Start Preferences panel to view or edit the proxy configuration. To do this, launch Application Manager, either by clicking the desktop icon (Microsoft Windows), or type **./javaws** in the Java Web Start installation directory (Solaris Operating Environment and Linux), and then select **Edit> Preferences**.

If you fail to change these settings, you may encounter installation issues regarding a version mismatch. If this occurs, clear your Java cache and retry.

Using a RSA Version 1 Key for SSH Following an Upgrade

For security reasons, NX-OS Release 4.2(1b) does not support RSA version 1 keys. As a result, if you upgrade to NX-OS Release 4.2(1b) from an earlier version that did support RSA version 1 keys, and you had configured an RSA version 1 key for SSH, then you will not be able to log in through SSH following the upgrade.

If you have an RSA version 1 key configured for SSH, before upgrading to NX-OS Release 4.1(3a), follow these steps:

Step 1 Disable SSH.

Step 2 Create RSA version 2 DSA keys.

Step 3 Enable SSH.

Step 4 Delete any RSA version 1 keys on any remote SSH clients and replace the version 1 keys with the new version 2 keys from the switch.

Proceed with the upgrade to NX-OS Release 4.2(1b).

If you upgrade before disabling SSH and creating RSA version 2 keys, follow these steps:

Step 1 Open a Telnet session and log in through the console.

Step 2 Use the **no feature ssh** command to disable SSH.

Step 3 Use the **ssh key rsa 1024** command to create RSA version 2 keys.

Step 4 Use the **feature ssh** command to enable SSH.

CFS Cannot Distribute All Call Home Information

In MDS NX-OS Release 4.2(1b), CFS cannot distribute the following Call Home commands that can be configured with the **destination-profile** command:

- **destination-profile** *profile_name* **transport-method**

- **destination-profile** *profile_name* **http**

The output of the **show running-config callhome** command shows configured Call Home commands:

```
switch# show running-config callhome
version 4.1(3)
callhome
email-contact abc@cisco.com <mailto:abc@cisco.com>
phone-contact +14087994089
streetaddress xyxxyx
distribute
destination-profile testProfile
destination-profile testProfile format XML
no destination-profile testProfile transport-method email
destination-profile testProfile transport-method http
destination-profile testProfile http https://xyz.abc.com
destination-profile testProfile alert-group all
transport email smtp-server 64.104.140.134 port 25 use-vrf management
transport email from abc@cisco.com <mailto:abc@cisco.com>
```

```
enable
commit
```

When you attempt to apply these commands in the ASCII configuration, the following commands fail:

```
no destination-profile testProfile transport-method email
destination-profile testProfile transport-method http
destination-profile testProfile http https://xyz.abc.com
```

To work around this issue, use these commands after the **commit** command.

Availability of F Port Trunking and F Port Channels

Trunking F ports and trunking F port channels are not supported on the following MDS 9000 components:

- DS-C9134-K9, Cisco MDS 9134 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch
- DS-C9124-K9, Cisco MDS 9124 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch

For configuration information, refer to the "Configuring Trunking" section in the *Cisco MDS 9000 NX-OS Interfaces Configuration Guide*.

Reserved VSAN Range and Isolated VSAN Range Guidelines

On an NPV switch with a trunking configuration on any interface, or on a regular switch where the **feature fport_channel_trunk** command has been used to enable the Trunking F port channels feature, follow these configuration guidelines for reserved VSANs and the isolated VSAN:

- If trunk mode is on for any of the interfaces or NP port channel is up, the reserved VSANs are 3040 to 4078, and they are not available for user configuration.
- The Exchange Virtual Fabric Protocol (EVFP) isolated VSAN is 4079, and it is not available for user configuration.

The following VSAN IDs are assigned in the Fibre Channel Framing and Signaling (FC-FS) interface standard:

VF_ID Value	Value Description
00h	Do not use as a Virtual Fabric Identifier.
001h ... EFFh	Available as a Virtual Fabric Identifier.
F00h ... FEEh	Reserved.
FEFh	Control VF-ID (see Fibre Channel Link Services (FC-LS) and Fibre Channel Switch Fabric Generation 4 (FC-SW-4) standards).
FF0h ... FFEh	Vendor specific.
FFFh	Do not use as a Virtual Fabric Identifier.
FEFh = 4079	—

Applying Zone Configurations to VSAN 1

In the setup script, you can configure system default values for the default-zone to be permit or deny, and you can configure default values for the zone distribution method and for the zone mode.

These default settings are applied when a new VSAN is created. However, the settings will not take effect on VSAN 1, because it exists prior to running the setup script. Therefore, when you need those settings for VSAN 1, you must explicitly use the following commands:

- **zone default-zone permit** *vsan 1*
- **zoneset distribute full** *vsan 1*
- **zone mode enhanced** *vsan 1*

RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules

An inter-switch link (ISL) that is enabled for Cisco TrustSec (CTS) encryption must be brought up in non-CTS mode to support remote SPAN (RSPAN) traffic on the following modules:

- DS-X9248-96K9: Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module
- DS-X9224-96K9: Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module
- DS-X9248-48K9: Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module

If the ISL link is brought up with CTS enabled, random packet drops of both RSPAN traffic and normal traffic will occur on the receiver port switch.

Saving Copies of the Running Kickstart and System Images

After you upgrade to MDS NX-OS Release 4.2(1b), you are not allowed to delete, rename, move, or overwrite the kickstart and system images that are in the current system bootvar settings on an active or standby MDS Supervisor-2 module on any Cisco MDS 9500 Series switch. This restriction does not apply to the integrated supervisor module on the MDS 9200 and MDS 9100 series switches.

Configuring Buffer Credits on a Generation 2 or Generation 3 Module

When you configure port mode to auto or E on a Generation 2 module, one of the ports will not come up for the following configuration:

- Port Mode: auto or E for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E on a Generation 3 module, one or two of the ports will not come up for the following configuration:

- Port Mode: auto or E for the first half of the ports, the second half of the ports, or for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E for all ports in the global buffer pool, you need to reconfigure buffer credits on one or more of the ports. The total number of buffer credits configured for all the ports in the global buffer pool should be reduced by 64.

Caveats

This section lists the open and resolved caveats for this release. Each caveat has a link to the Bug Search Tool, where you can find details.

Resolved Caveats in Cisco MDS NX-OS Release 5.2(8i)

Table 9   Cisco MDS NX-OS Release 5.2(8i) Resolved Caveats

Identifier	Description
CSCur53431	IVR zones missing after IVR zoneset activation/commit.
CSCuw84708	Evaluation of n9k, n3k, mds, n7k and n5k infra for NTP_October_2015.
CSCuy07280	Evaluation of N3k,N5k,N7k,N9k for OpenSSL January 2016.
CSCux41326	Evaluation of NX-OS for OpenSSL December 2015 vulnerabilities.
CSCuw03144	OpenSSH: Evaluation of Multiple OpenSSH CVEs for NX-OS.
CSCuc37616	SNMPd crashed on ACSII replay of config file.
CSCux86332	N7K/N6K/N9K/N3K January 2016 OpenSSH Vulnerabilities.
CSCue52901	MDS9000 Gen.4 Module in Failure state after ISSU due to Linecard manager.
CSCuz11494	FC Port-channel will not come up with UCS OUI 00:c8:8b.
CSCuy67727	Send LS_ACC for a LOGO that is not logged in on the interface.
CSCuy78337	Multiple Vulnerabilities Fix in 528h (OpenSSH, SSL, NTPd).

Open Caveats in Cisco MDS NX-OS Release 5.2(8i)

Table 10   Cisco MDS NX-OS Release 5.2(8i) Open Caveats

DDTS Number	Description
CSCue31727	User with priv-14 role does not inherit rules from priv-0 to priv-13.
CSCun82498	Port-Monitor delta threshold traps not sent after port goes down or flaps.
CSCue48324	Radius/tacacs+ users unable to login after upgrading - 'access denied'
CSCup69479	System default F mode causes FCIP tunnel to drop frames.
CSCuz89940	N7K/N5K/N6K/N2K/MDS IPv6 neighbor discovery packet processing behavior.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the documents listed in this section. To find a document online, access the following URL:

http://www.cisco.com/en/US/products/ps5989/tsd_products_support_series_home.html

The documentation set for Cisco Prime Data Center Network Manager is available from the following URL:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

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 Guides

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

Command-Line Interface

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.