



Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.2(2d)

Release Date: April 25, 2012

Part Number: OL-25090-04 J0

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 48.

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

[Table 1](#) shows the on-line change history for this document.

Table 1 **Online History Change**

Revision	Date	Description
A0	April 25, 2012	Created the release notes.
B0	May 2, 2012	<ul style="list-style-type: none">• Changed the status of caveat CSCtz09636 from Open to Resolved.• Added a Note to the “FICON Supported Releases and Upgrade Paths” section.
C0	May 7, 2012	Revised the description of caveat CSCty85364 .
D0	May 24, 2012	Revised the description of caveat CSCty85364 .
E0	June 25, 2012	Added open caveat CSCua61044 .
F0	August 8, 2012	Removed the “Upgrading to Cisco NX-OS Release 5.2 from Release 5.0(8)” section.
G0	August 29, 2012	Added M91S2K9-5.2.2d for the MDS 9134 and MDS 9124 switches to Table 2 .
H0	September 28, 2012	Updated the “Deprecated Features” section.



Table 1 **Online History Change**

Revision	Date	Description
I0	November 8, 2012	Added the “ NPE Software Images ” section.
J0	February 13, 2013	Updated the “ New Features in Cisco MDS NX-OS Release 5.2 ” section to include new features from earlier 5.2 releases.

Contents

This document includes the following:

- [Introduction](#), page 2
- [Components Supported](#), page 2
- [MDS 9000 Chassis and Module Support](#), page 9
- [Software Download Process](#), page 13
- [Upgrading Your Cisco MDS NX-OS Software Image](#), page 16
- [Downgrading Your Cisco MDS SAN-OS Software Image](#), page 20
- [Product information about Cisco MDS 9000 NX-OS software is available at this link:](#), page 24
- [Licensed Cisco NX-OS Software Packages](#), page 27
- [Deprecated Features](#), page 28
- [Limitations and Restrictions](#), page 29
- [Caveats](#), page 35
- [Related Documentation](#), page 48
- [Obtaining Documentation and Submitting a Service Request](#), page 50

Introduction

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 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 Software is fully interoperable with earlier Cisco SAN-OS versions and enhances hardware platform and module support.

Components Supported

[Table 2](#) lists the NX-OS software part numbers and hardware components supported by the Cisco MDS 9000 Family.

**Note**

For the latest information about supported transceivers, see the [Cisco MDS 9000 Family Pluggable Transceivers](#) data sheet.

Table 2 *Cisco MDS 9000 Family Supported Software and Hardware Components*

Component	Part Number	Description	Applicable Product
Software	M95S2K9-5.2.2d	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-5.2.2d	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M91S3K9-5.2.2d	MDS 9148 Supervisor/Fabric-3 NX-OS software	MDS 9148 Switch
	M91S2K9-5.2.2d	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9134 Switch and MDS 9124 Switch

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Licenses	M9500SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9500 Series only
	M9222ISSE1K9	Storage Services Enabler License	MDS 9222i Switch only
	M9200SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9500 Series only
	M9222IDMMK9	Data Mobility Manager License for Cisco MDS 9222i	MDS 9222i Switch
	M92DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9500 Series only
	M9222IDMMTSK9	Data Mobility Manager — Time Limited to 180 days only	MDS 9222i Switch only
	M92DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9200 Series only
	M92SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9500 Series only
	M92SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9200 Series only
	M95IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9200 Series only
	M95IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9500 Series only
	M9222IIOA	Cisco I/O Accelerator License for Cisco MDS 9222i base switch	MDS 9222i Switch only
	M92EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9200 Series only
	M95EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9500 Series only
M9200XRC	Cisco XRC Acceleration	MDS 9200 Series only	
M9500XRC	Cisco XRC Acceleration	MDS 9500 Series only	

Table 2 *Cisco MDS 9000 Family Supported Software and Hardware Components (continued)*

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	Cisco MDS 9513 Multilayer Director (13-slot multilayer director with 2 slots for Supervisor-2 modules, with 11 slots available for switching modules — SFPs sold separately)	MDS 9513 Switch
	DS-C9509	Cisco MDS 9509 Multilayer Director (9-slot multilayer director with 2 slots for Supervisor modules, with 7 slots available for switching modules — SFPs sold separately)	MDS 9509 Switch
	DS-C9506	Cisco MDS 9506 Multilayer Director (6-slot multilayer director with 2 slots for Supervisor modules, with 4 slots available for switching modules — SFPs sold separately)	MDS 9506 Switch
	DS-C9222i-K9	Cisco MDS 9222i Multilayer Fabric Switch (3-rack-unit (3RU) semimodular multilayer fabric switch with 18 4-Gbps Fibre Channel ports, 4 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9222i Switch
	DS-C9148-K9	Cisco MDS 9148 48-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 48 8-Gbps Fibre Channel ports)	MDS 9148 Switch
	DS-C9134-K9	Cisco MDS 9134 34-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 32 4-Gbps and 2 10-Gbps Fibre Channel ports)	MDS 9134 Switch
	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
Supervisor Modules	DS-X9530-SF2-K9	Cisco MDS 9500 Series Supervisor-2 Module	MDS 9500 Series
	DS-X9530-SF2A-K9	Cisco MDS 9500 Series Supervisor-2A Module	MDS 9500 Series

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Switching Modules	DS-X9112	Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9124	Cisco 24-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9148	Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series Mds 9200 Series
	DS-X9704	Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series MDS 9200 Series
	DS-X9224-96K9	Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-96K9	Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-48K9	Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series MDS 9222i Switch
	DS-X9708-K9	Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) Module	MDS 9500 Series
	DS-X9232-256K9	Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module	MDS 9500 Series
	DS-X9248-256K9	Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module	MDS 9500 Series
Services Modules	DS-X9316-SSNK9	Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16) — 16 fixed 1-Gbps Ethernet ports, plus 4 service engines that support 16 Gigabit Ethernet IP storage services ports.	MDS 9500 Series MDS 9222i Switch
	DS-X9304-18K9	Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) — 18-port, 4-Gbps Fibre Channel plus 4-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
External crossbar module	DS-13SLT-FAB1	Cisco MDS 9513 Switching Fabric 1 Module	MDS 9513 Switch
	DS-13SLT-FAB2	Cisco MDS 9513 Switching Fabric 2 Module	MDS 9513 Switch
	DS-13SLT-FAB3	Cisco MDS 9513 Switching Fabric 3 Module	MDS 9513 Switch

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Optics	SFP-10G-SR	10GBASE-SR SFP+ Module	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-10G-LR	10GBASE-LR SFP+ Module	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU1M	10GBASE-CU SFP+ cable 1 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU3M	10GBASE-CU SFP+ cable 3 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU5M	10GBASE-CU SFP+ cable 5 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-ACU7M	10GBASE-CU SFP+ active copper cable 7 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-ACU10M	10GBASE-CU SFP+ active copper cable 10 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP	DS-FC10G-SW	SFP+ optics (LC type) for 10-Gbps Fibre Channel for shortwave mode	32-port 8-Gbps Advanced Fibre Channel Module (DS-X9232-256K9), 48-port 8-Gbps Advanced Fibre Channel Module (DS-X9248-256-K9)
	DS-FC10G-LW	SFP+ optics (LC type) for 10-Gbps Fibre Channel for longwave mode	32-port 8-Gbps Advanced Fibre Channel Module (DS-X9232-256K9), 48-port 8-Gbps Advanced Fibre Channel Module (DS-X9248-256-K9)
	DS-SFP-FC8G-ER	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for extended reach (40 km reach)	MDS DS-X9200 Series switching modules, MDS 9148
	DS-SFP-FC8G-SW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for shortwave mode	MDS DS-X9200 Series switching modules
	DS-SFP-FC8G-LW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS DS-X9200 Series switching modules
	DS-SFP-FC4G-SW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for shortwave mode	MDS 9124, MDS 9134, MDS 9148, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-MR	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 4 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-LW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FCGE-SW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for shortwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FCGE-LW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for longwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-GE-T	SFP (RJ-45 connector) for Gigabit Ethernet over copper	MDS 9000 Series
Cisco Coarse Wavelength - Division Multiplexing (CWDM)	DS-CWDM-xxxx	CWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family
	DS-CWDM4Gxxxx	CWDM 4-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Dense Wavelength - Division Multiplexing (DWDM)	DWDM-X2-xx.xx	DWDM X2 SC optics for 10-Gbps Fibre Channel connectivity to an existing Ethernet DWDM infrastructure, with 15xx.xx nm wavelength, where xx.xx = 60.61, 59.79, 58.98, 58.17, 56.55, 55.75, 54.94, 54.13, 52.52, 51.72, 50.92, 50.12, 48.51, 47.72, 46.92, 46.12, 44.53, 43.73, 42.94, 42.14, 40.56, 39.77, 38.98, 38.19, 36.61, 35.82, 35.04, 34.25, 32.68, 31.90, 31.12, or 30.33	MDS 9500 Series MDS 9200 Series
	DWDM-SFP-xxxx	DWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 3033, 3112, 3190, 3268, 3425, 3504, 3582, 3661, 3819, 3898, 3977, 4056, 4214, 4294, 4373, 4453, 4612, 4692, 4772, 4851, 5012, 5092, 5172, 5252, 5413, 5494, 5575, 5655, 5817, 5898, 5979, or 6061nm	MDS 9000 Family
Add/Drop Multiplexer (ADM)	DS-CWDMOADM4A	4-channel CWDM optical ADM (OADM) module (Cisco CWDM 1470, 1490, 1510, or 1530 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDMOADM4B	4-channel CWDM OADM module (Cisco CWDM 1550, 1570, 1590, or 1610 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDM-MUX8A	ADM for 8 CWDM wavelengths	MDS 9000 Family
CWDM Multiplexer Chassis	DS-CWDMCHASSIS	2-slot chassis for CWDM ADMs	MDS 9000 Family
Power Supplies	DS-CAC-300W	300W AC power supply	MDS 9100 Series
	DS-C24-300AC	300W AC power supply	MDS 9124 Switch
	DS-CAC-845W	845W AC power supply for Cisco MDS 9200 Series	MDS9200 Series
	DS-CAC-3000W	3000W AC power supply for Cisco MDS 9509	MDS 9509 Switch
	DS-CAC-2500W	2500W AC power supply	MDS 9509 Switch
	DS-CDC-2500W	2500W DC power supply	MDS 9509 Switch
	DS-CAC-6000W	6000W AC power supply for Cisco MDS 9513	MDS 9513 Switch
	DS-CAC-1900W	1900W AC power supply for Cisco MDS 9506	MDS 9506 Switch
CompactFlash	MEM-MDS-FLD512M	External 512-MB CompactFlash memory for supervisor module	MDS 9500 Series
Port Analyzer Adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric	MDS 9000 Family
Smart Card Reader	DS-SCR-K9	Storage Media Encryption (SME) Smart Card Reader	MDS 9000 Family
Smart Card	DS-SC-K9	SME Smart Card	MDS 9000 Family

MDS 9000 Chassis and Module Support

Table 3 lists the MDS hardware chassis supported by Cisco MDS NX-OS 5.x.

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

Switch	NX-OS 5.x Support
MDS 9513	Yes
MDS 9509	Yes
MDS 9506	Yes
MDS 9222i	Yes
MDS 9148	Yes
Cisco MDS 8-Gb Fabric Switch for HP c-Class Blade System	Yes
MDS 9134	Yes ¹
MDS 9124	Yes ¹
Cisco MDS 4-Gbps Fabric Switch for HP c-Class BladeSystem	Yes ¹
Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter	Yes ¹

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

Table 4 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 5. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 3.x, see Table 6.

Table 4 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 ^{1,2}	No	No	No
DS-X9232-256K9	32-port 8-Gbps Advanced Fibre Channel Switching Module	Yes ¹	No	No	No
DS-X9248-256K9	48-port 8-Gbps Advanced Fibre Channel Switching Module	Yes ¹	No	No	No
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes ¹	Yes ³	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes ¹	Yes ³	No	No
DS-X9248-48K9	4/44-port Host Optimized 8-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes

Table 4 *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-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
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

1. Requires DS-13SLT-FAB3 or DS-13SLT-FAB2 in the MDS 9513.
2. Requires the Supervisor-2A module.
3. Requires DS-13SLT-FAB2 in the MDS 9513.

Table 5 *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 ¹	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 ²	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes ²	No	No
DS-X9248-48K9	4/44-port Host Optimized 8-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

Table 5 *Module Support Matrix for Cisco MDS NX-OS 4.x (continued)*

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
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

1. 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.
2. Requires DS-13SLT-FAB2 in the MDS 9513.

Table 6 lists the MDS hardware modules supported by Cisco MDS SAN-OS 3.x.

Table 6 *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 ¹	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 Optimized 8-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) ²	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

Table 6 **Module Support Matrix for Cisco MDS SAN-OS 3.x (continued)**

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
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

1. 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.
2. 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, page 13](#)
- [Determining Software Version Compatibility, page 13](#)
- [Downloading Software, page 14](#)
- [Selecting the Correct Software Image for an MDS 9100 Series Switch, page 15](#)
- [Selecting the Correct Software Image for an MDS 9200 Series Switch, page 15](#)
- [Selecting the Correct Software Image for an MDS 9500 Series Switch, page 15](#)
- [NPE Software Images, page 16](#)

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 7](#) 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 7 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(2d)	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
Cisco DCNM for SAN Software	Minimum NX-OS or SAN-OS Release	Tested NX-OS and SAN-OS Releases
DCNM for SAN Release 5.2(2c)	NX-OS Release 5.0(1a) or later	NX-OS Release 5.0(1a) and 5.0(4b)
	NX-OS Release 4.2(3) or later	NX-OS Release 4.2(3) and 4.2(7e)
	SAN-OS Release 3.3(5) or later	SAN-OS Release 3.3(5) and 3.3(5b)

Downloading Software

The Cisco MDS NX-OS software is designed for mission-critical high availability environments. To realize the benefits of 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	

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. 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, please 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 8](#).

Table 8 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
MDS 9148, Cisco MDS 8Gb Fabric Switch for HP c-Class BladeSystem	Filename begins with m9100-s3ek9

Selecting the Correct Software Image for an MDS 9200 Series Switch

The system and kickstart image that you use for an MDS 9200 series switch depends on which switch you use, as shown in [Table 9](#).

Table 9 Software Images for MDS 9200 Series Switches

Cisco MDS 9200 Series Switch Type	Naming Convention
MDS 9222i	Filename begins with m9200-s2ek9

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series are for switches with a Supervisor-2 module, as shown in [Table 10](#). Cisco NX-OS Release 5.x and Release 4.x do not support the Supervisor-1 module.

Table 10 Software Images for Supervisor Type

Cisco MDS 9500 Series Switch Type	Supervisor Module Type	Naming Convention
MDS 9513, 9509, and 9506	Supervisor-2 module Supervisor-2A module	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch. The following is sample output from the **show module** command on a Supervisor 2 module:

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---  -
...
...
7    0      Supervisor/Fabric-2        DS-X9530-SF2-K9     active *
8    0      Supervisor/Fabric-2        DS-X9530-SF2-K9     ha-standby
```

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:

- m9500-sf2ek9-kickstart-mz-npe.5.2.2.bin
- m9500-sf2ek9-mz-npe.5.2.2.bin

When downloading software, ensure that you select the correct software images for your 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:

- [Upgrading Guidelines Specific to NX-OS Release 5.2\(2d\)](#), page 16
- [Upgrading Guidelines Specific to NX-OS Release 5.2\(2d\)](#), page 16
- [General Upgrading Guidelines](#), page 17
- [Nondisruptive Upgrade Paths](#), page 18
- [FICON Supported Releases and Upgrade Paths](#), page 19



Note

Before you begin the upgrade process, review the list of chassis and modules that Cisco MDS NX-OS Release 5.2(2d) supports. See the [“MDS 9000 Chassis and Module Support”](#) section on page 9.

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/en/US/products/ps10495/prod_release_notes_list.html

Upgrading Guidelines Specific to NX-OS Release 5.2(2d)

Follow these guidelines when upgrading to Cisco MDS NX-OS Release 5.2(2d):

- Follow the upgrade path to NX-OS Release 5.2(2d) that is specified in [Table 11](#).
- Upgrade to NX-OS Release 5.2(x) before you install any Generation 4 module in an MDS 9500 Series switch. Generation 4 modules include the FCoE module and the 32-port and 48-port 8-Gbps Advanced Fibre Channel modules. NX-OS Release 5.2(x) is needed for the switch to recognize the new hardware.
- Perform a full switch reload on an MDS 9509 or MDS 9506 switch after you install NX-OS Release 5.2(1) and install any Generation 4 module, including the FCoE module. The switch reload is required for the new hardware to come up. Once you perform the switch reload, the fabric mode changes to support the Generation 4 hardware. Because of the changed fabric mode, you cannot subsequently perform a nondisruptive software downgrade from NX-OS Release 5.2(1). For additional information, see the [“Downgrading Guidelines Specific to NX-OS Release 5.2\(2d\)”](#) section on page 20
- Ensure that you have a Supervisor-2A module (DS-X9530-SF2A-K9) installed in a MDS 9500 Series switch if you plan to use the Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) (DS-X9708-K9).

- 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(1). 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-tunnel** *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(1). 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 re-establish all application 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(2d) in [Table 11](#).
- 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 11](#) for the nondisruptive upgrade path for all NX-OS and SAN-OS releases.

- **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MSM-18/4 module and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
- **FICON:** If you have FICON enabled, the upgrade path is different. See the [“FICON Supported Releases and Upgrade Paths”](#) section on page 19.

**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.

Nondisruptive Upgrade Paths

Use [Table 11](#) to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 5.2(2d). 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 11](#) applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and intelligent services traffic.

**Note**

Before upgrading to Cisco MDS NX-OS Release 5.2(2d) on a Cisco MDS 9509 or 9506 switch, see [Table 14](#) for specific guidelines.

**Caution**

Upgrading to Cisco NX-OS Release 5.2(2d) without first upgrading to Release 5.0(x) is not recommended and is not supported, and might result in configuration loss. If you are upgrading to Cisco NX-OS Release 5.2(2d) from any release other than Release 5.2(2a), Release 5.2(2) or Release 5.2(1) the only supported upgrade path to Release 5.2(2d) is from Release 5.0(x).

Table 11 **Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 5.2(2d)**

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
Release 5.2(1) and 5.2(2), and 5.2(2a)	Upgrade directly to NX-OS Release 5.2(2d).
All 5.0(x) releases	Upgrade directly to NX-OS Release 5.2(2d).
All 4.2(x) releases	<ol style="list-style-type: none"> 1. Upgrade to NX-OS Release 5.0(8a)¹. 2. Upgrade to NX-OS Release 5.2(2d).
All 4.1(x) releases	<ol style="list-style-type: none"> 1. Upgrade to NX-OS Release 5.0(8a). 2. Upgrade to NX-OS Release 5.2(2d).
SAN-OS:	
Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	<ol style="list-style-type: none"> 1. Upgrade to NX-OS Release 4.1(x) or 4.2(x). 2. Upgrade to NX-OS Release 5.0(8a). 3. Upgrade to NX-OS Release 5.2(2d).
Release 3.2(1a), all 3.2(x), 3.1(x), and 3.0(x) releases, and release 2.1(3), 2.1(2e), 2.1(2d), and 2.1(2b)	<ol style="list-style-type: none"> 1. Upgrade to SAN-OS Release 3.3(1c). 2. Upgrade to NX-OS Release 4.1(x) or 4.2(x). 3. Upgrade to NX-OS Release 5.0(8a). 4. Upgrade to NX-OS Release 5.2(2d).
Release 2.1(2), 2.1(1b), 2.1(1a), and 2.0(x)	<ol style="list-style-type: none"> 1. Upgrade to SAN-OS Release 2.1(2b), 2.1(2d), 2.1(2e), or 2.1(3). 2. Upgrade to SAN-OS Release 3.3(1c). 3. Upgrade to NX-OS Release 4.1(x) or 4.2(x). 4. Upgrade to NX-OS Release 5.0(8a). 5. Upgrade to NX-OS Release 5.2(2d).
Release 1.x	<ol style="list-style-type: none"> 1. Upgrade to SAN-OS Release 1.3(4a). 2. Upgrade to SAN-OS Release 2.1(2b). 3. Upgrade to SAN-OS Release 3.3(1c). 4. Upgrade to NX-OS Release 4.1(x) or 4.2(x). 5. Upgrade to NX-OS Release 5.0(8a). 6. Upgrade to NX-OS Release 5.2(2d).

1. Cisco NX-OS Release 4.2(7b) supports a direct upgrade to Release 5.2(2). Release 4.2(7b) is the *only* 4.2(x) release that supports a direct upgrade to Release 5.2(2). This direct upgrade path is available if you are using the open NX-OS Release 4.2(7b) software or the FICON-certified NX-OS Release 4.2(7b) software.

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 5.2(2d) is not a FICON-certified release.

[Table 12](#) lists the SAN-OS and NX-OS releases that are certified for FICON. Refer to the specific release notes for FICON upgrade path information.

Table 12 *FICON Supported Releases*

FICON Supported Releases	
NX-OS	Release 5.2(2)
	Release 4.2(7b)
	Release 4.2(1b)
	Release 4.1(1c)
SAN-OS	Release 3.3(1c)
	Release 3.2(2c)
	Release 3.0(3b)
	Release 3.0(3)
	Release 3.0(2)
	Release 2.0(2b)

Use [Table 13](#) to determine the nondisruptive upgrade path for FICON-certified releases. Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and follow the recommended path.

Table 13 *FICON Nondisruptive Upgrade Path*

Current Release with FICON Enabled	Upgrade Path
NX-OS Release 4.2(7b)	You can nondisruptively upgrade directly to NX-OS Release 5.2(2).
NX-OS Release 4.2(1b)	You can nondisruptively upgrade directly to NX-OS Release 4.2(7b).
NX-OS Release 4.1(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS Release 3.3(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS Release 3.2(2c), 3.0(3b), 3.0(3), and 3.0(2).	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).

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\(2d\)](#), page 20
- [General Downgrading Guidelines](#), page 21
- [NX-OS Release 5.2\(x\) and Release 5.0\(x\) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches](#), page 22

Downgrading Guidelines Specific to NX-OS Release 5.2(2d)

The following guideline applies to a downgrade from Cisco MDS NX-OS Release 5.2(2d):

- You cannot nondisruptively downgrade from NX-OS Release 5.2(2d) to NX-OS Release 5.0(x) if you installed NX-OS Release 5.2(2d) on an MDS 9509 or MDS 9506 switch and you installed a Generation 4 module in the switch and performed a full switch reload. The reason for this restriction is the change in fabric mode that occurs following the switch reload with the Generation 4 hardware installed. The downgrade will be disruptive, even if you remove the Generation 4 module prior to starting the downgrade.

If you do not install Generation 4 hardware or perform a full switch reload following the installation of NX-OS Release 5.2(2d) on an MDS 9509 or MDS 9506 switch, then you can nondisruptively downgrade to NX-OS Release 5.0(x).

- 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(2d) 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-tunnel *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 a software downgrade:

- Issue the system **no acl-adjacency-sharing** execute command to disable ACL adjacency usage on Generation 2 and Generation 1 modules. If this command fails, reduce the number of zones, IVR zones, TE ports, or a combination of these in the system and issue the command again.
- 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:
 - **FCoE:** Fibre Channel over Ethernet requires Cisco NX-OS Release 5.2(x). A downgrade from Release 5.2(x) disrupts and stops all FCoE traffic.
 - **Fibre Channel Ports:** Fibre Channel ports can be nondisruptively downgraded without affecting traffic on the ports. See [Table 15](#) for the nondisruptive downgrade path for all SAN-OS releases.
 - **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the downgrade is in progress.
 - **FICON:** If you have FICON enabled, the downgrade path is different. See the [“FICON Downgrade Paths”](#) section on [page 24](#).

NX-OS Release 5.2(x) and Release 5.0(x) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches

See the compatibility information in [Table 14](#) to determine if a downgrade to, or upgrade from Release 5.0(x) software is disruptive or nondisruptive on a Cisco MDS 9509 or 9506 switch.

Table 14 *NX-OS Release 5.2(x) and Release 5.0(x) Downgrade and Upgrade Matrix*

Downgrade Path on a Cisco MDS 9509 or 9506 Switch			
Current Release	Desired Release	Expected Behavior	Observed Behavior
5.2(2d) and above	5.2(2a) or 5.2(1)	Nondisruptive	Nondisruptive
5.2(2d) and below	5.0(7) or 5.0(8)	Disruptive	Disruptive
5.0(7) or 5.0(8)	5.0(1a), 5.0(1b)	Disruptive	Disruptive The user is expected to explicitly reload the switch using the reload command.
5.0(7) or 5.0(8)	5.0(4)	Nondisruptive	Nondisruptive
5.0(4)	5.0(1a)	Nondisruptive	Nondisruptive
5.0(1a), 5.0(1b), or 5.0(4)	4.2(x) or 4.1(x)	Nondisruptive	Nondisruptive

Upgrade Path on a Cisco MDS 9509 or 9506 Switch			
Current Release	Desired Release	Expected Behavior	Observed Behavior
5.2(1) or 5.2(2a)	5.2(2d)	Nondisruptive	Nondisruptive
5.0(7) or 5.0(8)	5.2(x)	Nondisruptive Support for Generation 4 modules is available.	Nondisruptive Support for Generation 4 modules is available.
5.0(1a), 5.0(1b), or 5.0(4)	5.2(x)	Nondisruptive Support for Generation 4 modules is not available.	Nondisruptive Support for Generation 4 modules is not available.

Use [Table 15](#) to determine the nondisruptive downgrade path from Cisco NX-OS Release 5.2(2d). Find the NX-OS or SAN-OS image that you want to downgrade to in the “To SAN-OS Release” column of the table and follow the steps in the order specified to perform the downgrade.



Note

The software downgrade information in [Table 15](#) applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and intelligent services traffic.

Table 15 **Nondisruptive Downgrade Path from NX-OS Release 5.2(2d)**

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
Release 5.2(1), 5.2(2), and 5.2(2a)	Downgrade directly from NX-OS Release 5.2(2d).
Release 5.0(1a), 5.0(1b), 5.0(4), 5.0(4b), 5.0(4c), and 5.0(4d)	Downgrade directly from NX-OS Release 5.2(2d) ^{1, 2, 3}
All 4.2(x) and 4.1(x) releases	<ol style="list-style-type: none"> 1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or 4.1(x).
SAN-OS:	
All 3.3(x) releases	<ol style="list-style-type: none"> 1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x).
All 3.2(x), 3.1(x), 3.0(x) releases, and all 2.1(x) releases.	<ol style="list-style-type: none"> 1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 3.2(x), Release 3.1(x), Release 3.0(x), or Release 2.1(x).
All 2.0(x) releases.	<ol style="list-style-type: none"> 1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 2.1(2x). 5. Downgrade to SAN-OS Release 2.0(x).
Release 1.x	<ol style="list-style-type: none"> 1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 2.1(2b). 5. Downgrade to SAN-OS Release 1.3(4a). 6. Downgrade to SAN-OS Release 1.x.

1. Before downgrading to NX-OS Release 5.0(8) or Release 5.0(7) on an MDS 9509 or MDS 9506 switch, see [“NX-OS Release 5.2\(x\) and Release 5.0\(x\) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches”](#) section on page 22.
2. If you install a Generation 4 module in an MDS 9509 or MDS 9506 switch and perform a full switch reload following the installation of NX-OS Release 5.2(2d), then you cannot nondisruptively download from NX-OS Release 5.2(2d) to NX-OS 5.0(x).
3. A downgrade from NX-OS Release 5.2(2d) to a release other than Release 5.2(1), 5.2(2), or 5.2(2a) disrupts and stops all FCoE traffic because FCoE requires Cisco NX-OS Release 5.2(x).

FICON Downgrade Paths

Table 16 lists the downgrade paths for FICON releases. Find the image release number that you want to downgrade to in the [To Release with FICON Enabled](#) column of the table and follow the recommended downgrade path.

Table 16 *FICON Downgrade Path*

To Release with FICON Enabled	Downgrade Path
NX-OS Release 4.2(7b)	You can nondisruptively downgrade directly from NX-OS Release 5.2(2)
NX-OS Release 4.2(1b)	You can nondisruptively downgrade directly from NX-OS Release 4.2(7b).
NX-OS Release 4.1(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.2(1b).
SAN-OS 3.3(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.1(1c).
SAN-OS 3.2(2c)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.2(2c).
SAN-OS 3.0(3b)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(3b).
SAN-OS 3.0(2)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(2).

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:

- [New Features in Cisco MDS NX-OS Release 5.2\(2d\), page 24](#)
- [New Features in Cisco MDS NX-OS Release 5.2\(2d\), page 24](#)
- [New Features in Cisco MDS NX-OS Release 5.2\(2\), page 25](#)
- [New Features in Cisco MDS NX-OS Release 5.2\(1\), page 25](#)
- [New Hardware in Cisco MDS NX-OS Release 5.2\(1\), page 26](#)

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(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 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.

SAN Extension over IP Package

The Cisco MDS 9000 SAN Extension over IP package allows the customer to use FCIP to extend SANs over wide distances on IP networks using the Cisco MDS 9000 family IP storage services. Refer to the Cisco MDS 9000 SAN Extension over IP 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.

Storage Media Encryption Package

The Cisco MDS 9000 Storage Media Encryption package enables encryption of data at rest on heterogeneous tape devices, virtual tape libraries, and disk arrays as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 Family switches and the Cisco DCNM for SAN application, enabling highly available encryption services to be deployed without rewiring or reconfiguring SANs, and allowing them to be managed easily without installing additional management software. Refer to the Cisco MDS 9000 Storage Media Encryption package fact sheet for more information. The Storage Media Encryption package is for use only with Cisco MDS 9000 Family switches.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility Manager package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or rewiring or reconfiguring SANs. Cisco DMM allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data verification, dual Fibre Channel fabric support, and management using Cisco DCNM for SAN provide a complete solution that greatly simplifies and eliminates most downtime associated with data migration. Refer to the Cisco MDS 9000 Data Mobility Manager package fact sheet for more information. The Data Mobility Manager package is for use only with Cisco MDS 9000 Family switches.

Storage Services Enabler Package

The Cisco MDS 9000 SSE package allows network-based storage applications and services to run on the Cisco MDS 9000 family SSMs, Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4), and Cisco MDS 9222i. Intelligent fabric applications simplify complex IT storage environments and help organizations gain control of capital and operating costs by providing consistent and automated storage management. Refer to the Cisco MDS 9000 SSE 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.

I/O Accelerator Package

The Cisco I/O Accelerator (IOA) package activates IOA on the Cisco MDS 9222i fabric switch, the Cisco MDS 9000 18/4 Multiservice Module (MSM-18/4), and on the SSN-16 module. The IOA package is licensed per service engine and is tied to the chassis. The number of licenses required is equal to the number of service engines on which the intelligent fabric application is used. The SSN-16 requires a separate license for each engine on which you want to run IOA. Each SSN-16 engine that you configure for IOA checks out a license from the pool managed at the chassis level. SSN-16 IOA licenses are available as single licenses.

XRC Acceleration License

The Cisco Extended Remote Copy (XRC) acceleration license activates FICON XRC acceleration on the Cisco MDS 9222i switch and on the MSM-18/4 in the Cisco MDS 9500 Series directors. One license per chassis is required. You must install the Mainframe Package and the SAN Extension over FCIP Package before you install the XRC acceleration license. The Mainframe Package enables the underlying FICON support, and the FCIP license or licenses enable the underlying FCIP support.

Deprecated Features

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

- [Zoning Features, page 29](#)
- [SNIA Common Information Model, page 29](#)

- [IVR Non-NAT Mode, page 29](#)

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](#).

IVR Non-NAT Mode

IVR non-NAT mode is not supported in Cisco NX-OS Release 5.2(x). If you have IVR non-NAT mode configured, see the [“Upgrading Guidelines Specific to NX-OS Release 5.2\(2d\)” section on page 16](#) for instructions on how to migrate to IVR NAT mode before upgrading to Cisco NX-OS Release 5.2(2d).

Limitations and Restrictions

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

- [FCoE Module, page 30](#)
- [IPv6, page 30](#)
- [User Roles, page 30](#)
- [Schedule Job Configurations, page 30](#)
- [Maximum Number of Zones Supported in Interop Mode 4, page 31](#)
- [InterVSAN Routing, page 31](#)
- [Java Web Start, page 31](#)
- [VRRP Availability, page 31](#)
- [Using a RSA Version 1 Key for SSH Following an Upgrade, page 31](#)
- [CFS Cannot Distribute All Call Home Information, page 32](#)
- [Availability of F Port Trunking and F Port Channels, page 32](#)
- [Reserved VSAN Range and Isolated VSAN Range Guidelines, page 33](#)

- [Applying Zone Configurations to VSAN 1, page 33](#)
- [Running Storage Applications on the MSM-18/4, page 33](#)
- [RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules, page 34](#)
- [I/O Accelerator Feature Limitations, page 34](#)
- [Support for FCIP Compression Modes, page 34](#)
- [Saving Copies of the Running Kickstart and System Images, page 34](#)
- [Configuring Buffer Credits on a Generation 2 or Generation 3 Module, page 34](#)
- [Features Not Supported on the Cisco MDS 9148 Switch, page 35](#)
- [PPRC Not Supported with FCIP Write Acceleration, page 35](#)
- [Configuring a Persistent FCID in an IVR Configuration with Brocade Switches, page 35](#)

FCoE Module

- In Cisco MDS NX-OS Release 5.2(x), you cannot install a FCoE module in a switch that is running DMM, SME, or IOA.
- Link traps for FCoE devices are sent only when a VFC interface flaps.

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.

InterVSAN Routing

When using InterVSAN Routing (IVR), it is recommended to enable Cisco Fabric Services (CFS) on all IVR-enabled switches. Failure to do so may cause mismatched active zone sets if an error occurs during zone set activation.

Java Web Start

When using Java Web Start, it is recommended 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 the 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, you should clear your Java cache and retry.

VRRP Availability

The Virtual Router Redundancy Protocol (VRRP) is not available on the Gigabit Ethernet interfaces on the MSM-18/4 module or module 1 of the MDS 9222i switch, even though it is visible on these modules. The feature is not implemented in the current release.

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 a RSA version 1 key for SSH, then you will not be able to log in through SSH following the upgrade.

If you have a 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** Issue the **no feature ssh** command to disable SSH.
 - Step 3** Issue the **ssh key rsa 1024** command to create RSA version 2 keys.
 - Step 4** Issue 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 xyxyx
> 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, issue 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

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

- DS-X9016, Cisco MDS 9000 2-Gbps16-Port Fibre Channel Switching Module

- DS-X9032, Cisco MDS 9000 2-Gbps 32-Port Fibre Channel Switching Module
- DS-X9032-14K9, Cisco MDS 9000 14/2-Port Multiprotocol Services Module (MPS-14/2)

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 issued to enable the Trunking F PortChannels feature, follow these configuration guidelines for reserved VSANs and the isolated VSAN:

- If trunk mode is on for any of the interfaces or NP PortChannel 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 issue the following commands:

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

Running Storage Applications on the MSM-18/4

The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) does not support multiple, concurrent storage applications. Only one application, such as SME or DMM, can run on the MSM-18/4 at a time.

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 packets drops of both RSPAN traffic and normal traffic will occur on the receiver port switch.

I/O Accelerator Feature Limitations

IOA does not support the following NX-OS features:

- F port trunking
- F port channeling
- IOA cannot be configured on flows in topologies that have devices with NPV and NPIV enabled. For example, IOA is not supported in a topology where a host logs in from a NPV edge switch and IOA is deployed on a NPV core switch for this host.

Support for FCIP Compression Modes

In Cisco NX-OS Release 4.2(1b) and later, FCIP compression mode 1 and compression mode 3 are not supported on the Cisco MSM-18/4 module and on the SSN-16 module.

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.

Features Not Supported on the Cisco MDS 9148 Switch

The Cisco MDS 9148 Multilayer Fabric Switch does not support the following NX-OS features:

- Remote Span
- Translative loop support
- FCC - no generation, quench reaction only
- FC-Redirect

In addition, the following features have these limits:

- VSANs - 31 maximum
- SPAN - 1 session maximum

PPRC Not Supported with FCIP Write Acceleration

IBM Peer to Peer Remote Copy (PPRC) is not supported with FCIP Write Acceleration.

Configuring a Persistent FCID in an IVR Configuration with Brocade Switches

The following information is relevant if you have a fabric that consists of Cisco MDS 9000 switches and Brocade switches, and the Cisco MDS switches are running either NX-OS Release 4.x or Release 5.x and Brocade is running FOS higher than 6.x. In an IVR configuration, when IVR NAT is enabled on a Cisco MDS 9000 switch, the device in the native VSAN should be configured with a persistent FCID. Assuming the FCID is 0xAABBCC, AA should be configured with the virtual IVR domain ID of the VSAN that contains the ISLs and BB should be configured in the following range:

- 1 through 64 if the Brocade switch is operating in native interop mode.
- 1 through 30 if the Brocade switch is operating in McData Fabric mode or McData Open Fabric Mode.

This configuration ensures that the devices connected to the Cisco MDS 9000 switch can be seen in the name server database on the Brocade switch.

Caveats

This section lists the open and resolved caveats for this release. Use [Table 17](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 17 *Open Caveats and Resolved Caveats Reference*

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2a)	5.2(2d)
Severity 2		
CSCtk60509	O	R
CSCtn72391	O	O
CSCto09131	O	R
CSCtq88900	O	O
CSCtr10877	O	O
CSCtr94463	O	R
CSCtw64713	O	O
CSCtx37102	O	R
CSCtx49190	O	R
CSCty01702	O	R
CSCty32238	O	R
CSCty68838	—	O
CSCty85364	O	R
CSCua61044	O	O
CSCum30306	O	O
CSCum82608	O	O
CSCuu76450	O	O
Severity 3		
CSCso67222	O	R
CSCtr26794	O	R
CSCtr29423	O	O
CSCtr50223	O	O
CSCtr55608	O	O
CSCtu13335	O	R
CSCtx17833	O	R
CSCty57144	O	O
CSCty97827	O	O
CSCtz09636	O	R
CSCtz10052	O	R
CSCtz14368	O	R
CSCtz15891	O	R
CSCtz21642	O	R
CSCtz25933	O	O

Table 17 *Open Caveats and Resolved Caveats Reference (continued)*

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2a)	5.2(2d)
CSCu122781	O	O
CSCuw06365	O	O
Severity 4		
CSCtz09820	O	O
CSCtz40700	O	O
CSCtz40745	O	O
CSCtz42028	O	R
Severity 6		
CSCtw84571	O	R

Resolved Caveats

- CSCtk60509

Symptom: A SANTap DPP may cause CRC errors in a multiple FE/BE VSAN setup with heavy I/O load.

This symptom might be seen when SANTap is running on a Cisco MDS 9000 MSM-18/4 module or Cisco MDS 9222i base module with multiple a FE/BE VSAN configuration. There is a heavy I/O load on both VSANs

Workaround: This issue is resolved.

- CSCto09131

Symptom: A DPP failure causes the MSM to reload. The **show cores** command shows the following output:

```
switch# show cores
Module-num      Instance-num    Process-name    PID            Core-create-time
-----
4                1              sb_part.0.0.0  12350000      Jul 11 14:45
4                1              ps_stap        1458          Jul 11 14:46
4                1              sb_part.0.0.1  12350100      Jul 11 14:46
4                1              sb_part.0.0.2  12350200      Jul 11 14:46
```

```
Signatures in the bt
#1 0x103a2360 in ssram_malloc () at
../platform/storage/las/linecard/dpp/isapi/octeon/sys/mem_xse.c:47
```

Workaround: This issue is resolved.

- CSCtr94463

Symptom: An FCIP engine fails and all FCIP links that are attached to that engine are brought down and up.

This issue is rare and has only been seen in one FICON environment with a triangular topology and both compression and FICON Tape Acceleration are enabled.

Workaround: This issue is resolved.

- CSCtx37102

Symptom: The FSPF route flaps every two seconds. The output of the **show system internal rib sync** command shows the following:

```

1  0000c702  update  add    130  cb0000 ff0000  Sun Jan 15 17:10:14 2012
2  0000c703  update  delete 130  cb0000 ff0000  Sun Jan 15 17:10:16 2012
3  0000c704  update  add    130  cb0000 ff0000  Sun Jan 15 17:10:18 2012
4  0000c705  update  delete 130  cb0000 ff0000  Sun Jan 15 17:10:19 2012
5  0000c706  update  add    130  cb0000 ff0000  Sun Jan 15 17:10:21 2012
6  0000c707  update  delete 130  cb0000 ff0000  Sun Jan 15 17:10:23 2012

```

Switch1:

FSPF Link State Database for VSAN 130 Domain 0xcb(203)

```

LSR Type           = 1
Advertising domain ID = 0x0d(13)
External LSR advertised by local switch
LSR Age           = 0
LSR Incarnation number = 0x80003e9d
LSR Checksum      = 0xfb1a
Number of links   = 1

```

NbrDomainId	IfIndex	NbrIfIndex	Link Type	Cost
0x0d(13)	0x0010cb0d	0x00100dcb	1	30001

Switch2:

FSPF Link State Database for VSAN 130 Domain 0xcb(203)

```

LSR Type           = 1
Advertising domain ID = 0x23(35)
External LSR advertised by local switch
LSR Age           = 0
LSR Incarnation number = 0x80003f2c
LSR Checksum      = 0x3785
Number of links   = 3

```

NbrDomainId	IfIndex	NbrIfIndex	Link Type	Cost
0x21(33)	0x0010cb21	0x001021cb	1	30001
0x0f(15)	0x0010cb0f	0x00100fcb	1	30001
0x23(35)	0x0010cb23	0x001023cb	1	30001

This symptom might be seen when you disable IVR and there is an E link down or the switch reloads at the same time. A stale FSPF route is left in the FSPF database, which causes virtual domain flaps.

Workaround: This issue is resolved.

- CSCtx49190

Symptom: Cisco MDS Storage Media Encryption (SME) tape keys are incorrectly purged, which causes the tapes to be unreadable because the keys are no longer in the database.

This symptom might be seen following a DPP failure that is shown as a port software failure:

```

%IPS_SB_MGR-SLOT12-2-PORT_SOFTWARE_FAILURE: Port software failure, module 12
port 1
%IPS_SB_MGR-SLOT12-2-PORT_SOFTWARE_FAILURE: Port software failure, module 12
port 2
%IPS_SB_MGR-SLOT12-2-PORT_SOFTWARE_FAILURE: Port software failure, module 12 port 3
%IPS_SB_MGR-SLOT12-2-PORT_SOFTWARE_FAILURE: Port software failure, module 12
port 4

```

Workaround: This issue is resolved.

- CSCty01702

Symptom: FCIP interfaces go down and stay down. The output of the **show logging log** command shows the following output:

```

switch# show logging log
%IPS-SLOT2-3-RED_PACKET_DROPS: Congestion detected on GigabitEthernet port (buffer pool size: ...)

```

```
%PORT-5-IF_PORT_QUIESCE_FAILED: Interfacefcip51 port quiesce failed due to failure reason: Force Abort
Due to Link
Failure (0xa2)
```

This symptom might be seen in NX-OS Release 4.2(1) through Release 5.2(2a) when IPSec is enabled and configured for FCIP.

Workaround: This issue is resolved.

- CSCty32238

Symptom: On certain hardware, certain Cisco MDS 9000 Series features and applications do not work. These include IVR, IOA, DMM, SME, fcflow, and SPAN.

The following devices with hardware revision 1.5 are affected by this issue:

- DS-X9248-96K9, 48-port 8-Gbps Fibre Channel Switching Module
- DS-X9248-48K9, 4/44-port host-optimized 8-Gbps Fibre Channel Switching Module
- DS-X9224-96K9, 24-port 8-Gbps Fibre Channel Switching Module

The following devices with hardware revision 1.0 are affected by this issue:

- DS-X9304-18K9, 18/4-Port Multiservice Module (MSM-18/4)
For this module, the affected version is 73-14372-01A0 hardware version 1.0 (due to the new 73-number)
- DS-C9222i-K9, Cisco MDS 9222i Multilayer Fabric Switch
For this switch, the affected version is 73-14373-01A0 hardware version 1.0 (due to the new 73-number)

For the DS-X9248-96K9, DS-X9248-48K9 and DS-X9224-96K9 modules, the output of the **show module** command indicates whether or not the device is affected.

```
switch# sh mod 2
Mod  Ports  Module-Type                Model                Status
---  ---
2    24      1/2/4/8 Gbps FC Module    DS-X9224-96K9       ok

Mod  Sw          Hw          World-Wide-Name(s) (WWN)
---  ---
2    5.2(1)      <B>1.0</B>   20:41:00:0d:ec:24:f4:c0 to
20:58:00:0d:ec:24:f4:c0
```

In the preceding output, the device is hardware revision 1.0 and therefore not affected.

For the DS-X9304-18K9 and the DS-C9222i-K9, the **show module** command might indicate hardware version 1.0 due to new part numbers; however the **show sprom module** command shows the affected parts.

```
switch# sh mod 9
Mod  Ports  Module-Type                Model                Status
---  ---
9    22      4x1GE IPS, 18x1/2/4Gbps FC Module    DS-X9304-18K9       ok

Mod  Sw          Hw          World-Wide-Name(s) (WWN)
---  ---
9    5.2(1)      1.0        22:01:00:0d:ec:25:e9:80 to 22:12:00:0d:ec:25:e9:80

Mod  MAC-Address(es)                Serial-Num
---  ---
9    00-1a-e2-03-4c-5c to 00-1a-e2-03-4c-64  JAE1131SCBW

switch# sh sprom module 9 1 |egrep "Part|Serial"
Serial Number   : JAE1131SCBW
Part Number     : 73-10688-06      <-- Not 73-14372-01 so h/w ver 1.0 is OK
Part Revision   : A0
```

Workaround: This issue is resolved.

- CSCty85364

Symptom: Devices on an NPV switch with a trunked uplink to the core NPIV switch lose connectivity to other devices after zone configuration changes.

Conditions: This issue occurs after a zone set activation and only when all of the following conditions are true:

- The switch is running NX-OS Release 5.2(1), Release 5.2(2), or Release 5.2(2a)
- The F-port on the NPIV switch is located on an MDS 9000 48 port 8-Gbps Advanced Fibre Channel module (DS-X9248-256K9) or on an MDS 9000 32 port 8-Gbps Advanced Fibre Channel module (DS-X9232-256K9).
- The F-port carries multiple VSANs.
- The zone set activation is for a VSAN that is trunked to the NPV switch.

Workaround: This issue is resolved in NX-OS Release 5.2(2d). However, upgrading to Release 5.2(2d) after you encounter this issue in an earlier 5.2(x) release does not completely resolve the issue; it only prevents the issue from reoccurring.

When you encounter this issue, the ACL TCAM programming is deleted. To recover from this situation, you must restore the communication between the devices by restoring the ACL TCAM programming.

Recovery Steps:

To restore the ACL TCAM programming, do one of the following:

- Reload the DS-X9232-256K9 module or DS-X9248-256K9 module.
- Enter the **shut** command followed by the **no shut** command on the host and target ports that have lost connection.
- Reload the hosts that have lost the targets.



Note If you have already upgraded to NX-OS Release 5.2(2d) without completing the recovery steps in Release 5.2(1), 5.2(2), or 5.2(2a), you must complete the recovery steps because the ACL entries that were deleted are not reprogrammed during the ISSU.

Workaround Steps:

If upgrading to NX-OS Release 5.2(2d) is not an option, you can work around this issue by following these steps:

- Attach multiple F-ports between the NPV and NPIV switches and allocate one VSAN to each F-port.
- Move the F-port uplink to a module that is not a DS-X9248-256K module or a DS-X9232-256K module.

- CSCso67222

Symptom: In very rare circumstances in IVR NAT configurations, it is possible that devices from two or more VSANs stop communicating. The root cause is there are stale device entries in IVR vdri-fsm, which cause IVR DEP and PVM to get stuck, which prevents the name server from registering the devices.

There is a stale device entry in vdri-fsm device list:

```
switch4# sh ivr internal vdri-fsm vsan 130 domain 203
```

```
VDRI FSM: A=1:V=130:D=0xcb(203)
```

```
Native VSAN/AFID = 111/1 Cur State: LSR_OWNER
```

```
Number of Devices Advertised: 1
```

```
FCID: 0xcb7f98 WWN=10:00:00:00:c9:7a:06:4c PV Pending: Add=No Del=No <---offline device, pwn not in ivr zoneset and fcns database
```

```
PNAT
```

```
switch1# sh ivr internal pnat vdom-info vsan 130
```



```

IVR2 PNAT: Virtual domain info for 1:130:203 is_owner=false, owner_dom=13, local_dom=15
ID: VDOM-1:130:203
switch2# sh ivr internal pnat vdom-info vsan 130
IVR2 PNAT: Virtual domain info for 1:130:203 is_owner=false, owner_dom=13, local_dom=35
ID: VDOM-1:130:203
switch3# sh ivr internal pnat vdom-info vsan 130
IVR2 PNAT: Virtual domain info for 1:130:203 is_owner=false, owner_dom=13, local_dom=33
ID: VDOM-1:130:203
switch4# sh ivr internal pnat vdom-info vsan 130
NONE

```

There should be outputs like the following:

```
is_owner=true, owner_dom=13, local_dom=13
```

Therefore, at switch2 and switch3, the system keeps trying with switch4, but cannot get an OXID. The counter below shows the retry count.

```

switch2# show ivr internal dep vsan 130
Internal information for DEP FSM
-----
vsan      domain  nh          status  sync_status req i/f
  130    0xcb(203)  111        NONE    FCID_RW 9955 <-----Missing OXID here
Number of DEP entries : 1

```

```

switch1# show ivr internal dep vsan 130
Internal information for DEP FSM
-----
vsan      domain  nh          status  sync_status req i/f
  130    0xcb(203)  111        NONE    FCID_RW 10034<-----Missing OXID here

```

The output should be like the following:

```
12 0x23(35) 211 ALL_DONE OXID|FCID_RW 0 [ fc5/1 fc9/2 fc4/2 fc1/8 fc6/1 fc5/2 fc2/8 fc6/2
fc3/8 fc1/10 fc4/8 fc2/10 fc4/10 fc3/10 ]
```

```

switch2# show ivr internal pvm dom 203 vsan 130
AFID:1 Vsan:130 Virtual domain:203
Domains:13,15,33,35
Domains added to route LSR:13,15 <----- should have full list 13,15,33,35
Flags:0x3 (ROUTE_ADDED )

Device List

Port WWN:10:00:00:00:xx:yy:zz:aa
Domains with rewrite completed:13,15,33,35
Domains with registered NS info:13,15 <----- should have full list 13,15,33,35
Flags:0x3 (INITIAL_SYNC RSCN_ONLINE_SENT )

```

Stale domain entry: on the LSR_owner switch that has the stale device in vdri, the zone database may also have an inconsistent domain while the peer switch does not.

```

switch# show zone internal vsan 130

203(0xcb)

rib has both fspf and ivr entry
fspf      130  cb0000 ff0000  00 00  D P A  1  63  F  normal frm
  ivr 13:203 Domain 0xcb(203)
ivr       130  cbffff ffffff  00 00  R P A  1  0  F  normal frm
  sup-fc0

```

This symptom might be seen under the following conditions:

- A version of software between SAN-OS Release 3.2(x) and NX-OS Release 4.1(x) is loaded on the switch.

- A device state change occurs due to a stimulus such as an F port down, E link flapping, VSAN suspend, or domain withdrawn.
- A device goes down or a domain goes down during an ISSU or switchover.

Workaround: This issue is resolved.

- CSCtr26794

Symptom: The **copy running-config startup-config** command should display an error if a VDC global configuration change is pending.

Workaround: This issue is resolved.

- CSCtu13335

Symptom: DMM is limited to five jobs per storage port.

Workaround: This issue is resolved.

- CSCtx17833

Symptom: The TSM application that runs through Storage Media Encryption (SME) feature on a Cisco MDS 9000 switch reports the following error message:

```
ANR8311E An I/O error occurred while accessing drive DRIVEx (/dev/rmtx) for READ operation, errno = 78.
```

This error results when the switch drops a small number of SCSI data frames at the very end of a large read exchange.

This symptom might be seen when the HBA for the TSM server is connected at 2-Gbps to the MDS 9000 switch.

Workaround: This issue is resolved.

- CSCtz09636

Symptom: New syslog messages do not get added to the log file on the supervisor and do not appear in the output of the **show logging log** command.

This symptom might be seen when the log has 0 bytes free, which can be seen with the **dir log:** command. In addition, the contents of log:startupdebug is updated about every 2 to 5 minutes or with every SNMP poll from an SNMP application like Cisco Fabric Manager or DCNM-SAN.

Workaround: This issue is resolved..

- CSCtz10052

Symptom: FICON Tape Acceleration VTD-to-RTD recalls fail.

Workaround: This issue is resolved.

- CSCtz14368

Symptom: Excessive bit errors on MDS generation 4 ports do not trigger the port to be shut down by the default bit error monitoring process.

This issue occurs only on ports on the 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) or on the 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9).

Workaround: This issue is resolved.

- CSCtz15891

Symptom: A Cisco MDS 9000 switch does not issue the following SFP warning and failure messages on Generation 4 modules:

```
%PORT-4-IF_SFP_WARNING: Interface fcx/y
%PORT-3-IF_SFP_ALARM: Interface fcx/y
```

This symptom might be seen only on the following modules:

- DS-X9232-256K9, Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module
- DS-X9248-256K9, Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module

Workaround: This issue is resolved.

- CSCtz21642

Symptom: Following an upgrade to NX-OS Release 5.2.(1), four ports went into error disabled state due to a failed validation. The transceiver was a non FC transceiver, and it failed FC compliance.

The output of the **show interface** command shows the following

```
switch# show interface
```

```
fc1/47 is down (Error Disabled - The transceiver has failed FC compliance)
  Port description <removed>
  Hardware is Fibre Channel, SFP is CWDM-1550

fc2/47 is down (Error Disabled - The transceiver has failed FC compliance)
  Port description <removed>
  Hardware is Fibre Channel, SFP is CWDM-1570
```

This symptom might be seen following an upgrade from SAN-OS Release 3.3(x) to Release NX-OS 4.2(x) and then to NX-OS 5.2(x).

After upgrade, the CWDM links using SFPs DS-CWDM-1550= or DS-CWDM-1570= were down. The links using SFPs DS-CWDM-1590= or DS-CWDM-1610= were still up.

Workaround: This issue is resolved.

- CSCtz42028

Symptom: The traps 1.3.6.1.4.1.9.9.276 and 1.3.6.1.6.3.1.1.5.3 send an incorrect “ifAdminStatus down” state.

This symptom might be seen only in the case of a link failure on an E, TE, or TF port.

Workaround: This issue is resolved.

- CSCtw84571

Symptom: When any previously configured LUN cannot be discovered, the IT nexus stays offline without informing the user about the discovery failure for the LUN.

This symptom might be seen when a report LUN failure on the target side causes the LUN discovery to fail.

Workaround: This issue is resolved.

Open Caveats

- CSCtn72391

Symptom: Following a switch reload or a software upgrade, the startup configuration occasionally does not display feature FCIP.

Workaround: Once the switch is completely up, copy the running configuration to the startup configuration by entering the **copy running-config startup-config** command.

- CSCtr10877

Symptom: Following an ISL flap that isolates some switches in the fabric (and the corresponding FCR peers) and then later merges them again, some FCR peers might get out of sync with the SSM switch FCR peer (that is, the FCR peer that owns a configuration) during the peer discovery phase. Consequently, some application flows might not come online, or might even get deleted.

Workaround: Enter the following supervisor commands on the problematic FCR peer, which will trigger this FCR peer to resync with the rest of the fabric, and force it to come out of the error state:

```
switch# test fc-redirect config sync-with-fabric
switch# test fc-redirect config sync-with-fabric all-peers
```

If more than one peer is affected by this issue, then additional steps are needed. If the application flows do not come online, then the application CLI commands need to be checked to verify that the flows did not get deleted. If they did, then the flows need to be recreated again through the application CLI commands or Cisco DCNM-SAN interface.

- CSCtw64713

Symptom: Occasionally, a 10-G ISL between a 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) or a 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9) and an older generation Cisco MDS 9000 module can take a long time to come up. The link can go into an error-disabled state.

Workaround: None.

- CSCty68838

Symptom: Periodic FCIP port flaps might occur when Tape Acceleration and IP compression are enabled and the MTU is configured at 9000. This situation might lead to a failure of an IPS core.

This symptom might be seen when the following configuration is applied to an FCIP tunnel:

- Tape Acceleration (TA) is enabled.
- Write Acceleration (required for TA) is enabled.
- IP compression is enabled.
- The MTU size is 9000.

Workaround:

This issue does not occur if TA is not configured and other parameters remain the same.

This issue does not occur if the MTU size of up to 2500 is configured and other parameters remain the same.

- CSCua61044

Symptom: A device that is attached to a Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9) or a Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) is not able to communicate with other devices.

This symptom occurs only when a port on the DS-X9248-256K9 or DS-X9232-256K9 module is zoned to more than 146 unique devices.

The following errors can be seen in the log of the DS-X9248-256K9 or DS-X9232-256K9 module:

```
switch# show process acלטcam internal errors
 1) Event:E_DEBUG, length:84, at 359632 usecs after Tue Jun 19 23:34:44 2012
    [109] Program rqst sync failed. Fwd-eng:0(IN) ifIndex: 0x1104000, status: 0x404e0005
 2) Event:E_DEBUG, length:65, at 359603 usecs after Tue Jun 19 23:34:44 2012
    [112] Failed: tcamwrap2_tcam_ssrām_write, 155 entries, errno: 28
```

Workaround: Reduce the number of devices that this port is zoned to to 146 devices or less, or connect the device that is attached to the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module or the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module to a different model module.

CSCtq88900

Symptom: In an SME or IOA deployment, if the number of H->T flows that are added exceeds 512, then subsequent disruptive platform events can leave an FCR unable to process interprocess (MTS) messages at a rate fast enough to support the scaled configuration. This situation can cause an MTS-buffers full condition in the FCR, which can result in unpredictable behavior. Some of the resulting errors may be unrecoverable, and may require a disruptive restart of the flows.

Workaround: Use CFS regions if a large number (greater than 512) of application flows need to be configured. CFS regions segment the FCR peer topology into manageable proportions.

- CSCtr29423

Symptom: Tape acceleration is not working with the Emulex CNA card. This issue can be seen because the Emulex CNA card uses the same OXID for all fast-path SCSI commands (read/write), which breaks tape acceleration logic for accelerating the read/write IOs.

Workaround: None.

- CSCtr50223

Symptom: On the MDS 9513 switch, when an MSM-18/4 module boots up, it sends a request to the supervisor module to mount the modflash on the MSM-18/4 module. If there is a timeout or error in response, the following syslog message displays:

```
2011 Jul 14 01:18:13 sw-dc5-br2-12 %LC_MNT_MGR-SLOT3-2-LC_MNT_MGR_ERROR: SUP mount failed. MTS receive
timeout
2011 Jul 14 01:19:06 sw-dc5-br2-12 %PROC_MGR-SLOT3-2-ERR_MSG: ERROR: PID 1144 (lc_mnt_mgr) exited
abnormally, exit status (0xa)
2011 Jul 14 01:19:06 sw-dc5-br2-12 %MODULE-2-MOD_MINORSWFAIL: Module 3 (serial: JAE1141ZB43) reported a
failure in service lc_mnt_mgr
```

This issue might be seen when the supervisor module is unusually busy and cannot process the mount request from the MSM-18/4 module, or the actual mount command on the supervisor takes a long time.

Workaround: Reload the MSM-18/4 module in the same slot/module where the modflash mount failed. A request will be sent to the supervisor to mount the modflash.

- CSCtr55608

Symptom: Following the insertion of the 32-port 8-Gbps Advanced Fibre Channel switching module (DSX9232-256K9), the following syslog message is displayed:

```
2011 Jul 16 05:35:00 emc-9513-II %SYSMGR-STANDBY-3-UNACCEPTABLE_WAIT: Service "r
es_mgr", no response from System Manager after 10 seconds. Terminating.
```

This issue might be seen if you enter the **no install feature-set fcoe** command, then power down the 32-port 8-Gbps Advanced Fibre Channel switching module, and then insert the module again, which triggers the install feature-set fcoe command.

Workaround: None. This is not an operationally impacting issue because it happens on the standby supervisor, and the standby supervisor can successfully come up in spite of the syslog message.

- CSCuw06365

Symptom: An ISL does not initialize quickly across a DWDM connection. The link can take minutes, hours or even days to connect. Once connected, it is stable

Conditions: This issue only applies to DS-X9248-256K9 and DS-X9232-256K9 modules when connecting an ISL over a Tellabs 7100 DWDM path.

Workaround: None.

- CSCty57144

Symptom: The management interface on a Cisco MDS 9148 switch is 10/half after the switch reloads.

Workaround: Enter the **shut** command followed by the **no shut** command on the switch.

- CSCty97827

Symptom: Host-to-target connectivity across multihop connected switches is lost. The fcping fails between devices through a port channel.

This issue is extremely rare. The conditions for it may be created after a nondisruptive upgrade to Cisco NX-OS Release 5.2(x). However service disruption might not appear immediately on the affected port channel. The next time one or more members of the port channel flap, traffic loss could occur.

To verify if you have the potential to experience this issue, enter the commands shown in the following examples:

```
switch# show port-channel internal info interface port-channel 3
```

```
port-channel 3
channel      : 3   <<< channel_id
bundle      : 10  <<< normally, bundle_id = channel_id - 1
ifindex     : 0x4000002
pcport mode : 67108866
admin mode  : on
oper mode   : on
[...]
```

```
switch # show system internal fcfwd pemap
```

```
port-channel 3:
  IfIndex is 0x04000002      <<< last 3 nibbles
  Bundle-Index is 0x0000000a <<< last 3 nibbles are not equal
[...]
```

Regardless of the last three nibbles of the preceding indexes, this issue has been hit if the following output contains “pcm_reserv_bundle_id:Conflict,rsv a new one...”

```
switch# show port-channel internal event-history port-channel 1
```

```
29) Event: E_DEBUG at 487974 usecs after Thu Mar 22 19:44:26 2012
pcm_reserve_bundle_id:Conflict,rsv a new one.req_bundle=0x0,resp_bundle=0x1
```

Workaround: Flap the affected port channel by entering the **shut** command followed by the **no shut** command and confirm that the issue is no longer present. Note that bundle id is not going to change to channel_id-1, but the last 3 nibbles in IfIndex and Bundle-Index should match.

```
switch# show port-channel internal info interface port-channel 3
```

```
port-channel 3
channel      : 3
bundle      : 10
ifindex     : 0x4000002
pcport mode : 67108866
[...]
```

```
switch# show system internal fcfwd pemap
```

```
port-channel 3:
  IfIndex is 0x04000<B>00a</B>
  Bundle-Index is 0x00000<B>00a</B>
[...]
```

- CSCtz25933

Symptom: Some onboard logging statistics are not updated as frequently as required. These statistics are used only for debugging limited types of problems.

This symptom might be seen only on the 32-port 8-Gbps Advanced Fibre Channel module (DS-X9232-256K9) and the 48-port 8-Gbps Advanced Fibre Channel module (DS-X9248-256K9).

Workaround: None.

- CSCtz09820

In Generation 4 modules, the following errors might be observed. They are not a cause for concern to the normal operation of the hardware. These errors are logged in the onboard persistent log and can be viewed by entering the **show logging onboard exception-log** command after attaching to the module.

```
TBIRD_FWD_EBM_0_SER_PARITY_XXX : Informational
TBIRD_FWD_EBM_0_PACK0_EPR_DROP : Informational
TBIRD_FWD_EBM_1_PACK3_MISS_SOF : Informational
TBIRD_FWD_EBM_1_PACK0_MISS_EOP : Informational
TBIRD_FWD_EBM_1_PACK0_SF_TOO_SMALL : Informational
```

These errors are reported when there are internal correctible conditions encountered during operation, and the corrective action is taken. They do not necessarily indicate a problem with the switch or module.

The following error can occur in cases of corrupted frames in the ingress path (due to a bad cable or SFP). It does not necessarily indicate a problem with the switch hardware.

```
THB_IPA_IPA0_INTR_FLD_ERR_FROM_MEM : Warning
```

Workaround: None.

- CSCtz40700

Symptom: When a trunk link fails, the 1.3.6.1.4.1.9.9.289.1.3 trap has an incorrect link failure reason of “gracefully down.”

This symptom might be seen only when a link failure occurs on a E, TE, or TF port.

Workaround: Ignore the link down reason because the link down trap is valid.

- CSCtz40745

Symptom: A “VSAN down” trap is sent for VSAN 4094 when a trunk port goes down because the VSAN is not configured on the trunk.

This symptom might be seen only when a link down occurs on a E, TE, or TF port.

Workaround: Ignore the trap.

- CSCul22781

Symptom: After a supervisor switchover, a subsequent ISL flap results in one or more VSAN becoming isolated on the ISL.

Conditions: These issues only occur in situations after the supervisors fail over or a user-initiated switch over occurs (but not an in service switchover situation, ie ISSU/ISSD). The preconditions are created before the switchover by activating zone changes (such as adding or removing zones from a zoneset) and is more likely to occur on systems with very large zone configurations.

The symptoms described here can occur if zones are modified while a switch is running any NX-OS release 5.2(2) to 5.2(8c) (inclusive), and 6.2(1) to 6.2(5) (inclusive).

Workaround: Contact Cisco TAC for assistance clearing the condition nondisruptively.

- CSCum30306

Symptom: The security service crashes when configuring an SSH authentication key.

Configuring SSH keys multiple times within 10 minutes results in a HAP reset that resets the active supervisor.

Condition: This issue intermittently occurs when configuring an SSH authentication key.

Workaround: To avoid the supervisor reset, do not configure more than 2 SSH keys per 10 minutes.

- CSCum82608

Symptom: The full zoneset database in one or more VSANs may be empty after a supervisor switchover.

Conditions: This issue only occurs after the supervisors fail over or a user-initiated switch over occurs (but not an in service switchover situation, ie ISSU/ISSD). The precondition is created before the switchover by activating zone changes (such as adding or removing zones from a zoneset) and is more likely to occur on systems with very large zone configurations.

The symptom described here can occur if zones are modified while a switch is running any NX-OS release 5.2(2) to 5.2(8c) (inclusive), and 6.2(1) to 6.2(5) (inclusive).

Workaround: To recover from this condition follow these steps:

1.

[i] If the full zoneset db for the affected VSAN contains multiple zonesets (ie, inactive zonesets) follow these steps:

- a. add dummy zone to any zoneset in the full zoneset db for the vsan on a **neighbouring** switch, and then
- b. if zoning mode is basic distribute the change or if the zoning mode is enhanced commit the change, and then
- c. the dummy zone may be removed now and the zoneset redistributed/recommitted.

[ii] If the full zoneset db for the affected VSAN contains only a single zoneset (ie, no inactive zonesets) follow these steps:

- a. copy the active zoneset db to the full zoneset db on the **affected** switch (it is only necessary to copy zonesets for VSANs that have empty databases), For example:

```
switch# zone copy active-zoneset full-zoneset vsan 1-4093
```

2. In both cases, save the config on the **affected** switch after step 1, For example:

```
switch# copy running start
```

To recover from condition 2 (isolated ISL) contact Cisco TAC for assistance.

- CSCuu76450

Symptom: MDS fabric switch running in NPV mode fails to generate port-monitor alerts.

Condition: Applies to all MDS fabric switches running in NPV mode using port-monitor.

Applies to all versions prior to NX-OS 6.2(13).

Will occur only in the following conditions:

- After one or more upstream NP or TNP ports goes down and then back up.
- For each (T)NP port that flaps, one F port at the end of the range of ports will no longer be scanned for port-monitor counter events. For example, if the (T)NP port fc1/1 flaps then the last F port being used(ex. fc1/48) will no longer be scanned for port-monitor counter events.

Workaround: There are two workarounds, one temporary and one permanent:

1 - Contact the TAC and they can assist with killing the port-monitor process. Once the port-monitor process restarts, all ports will be once again scanned.

This is only temporary in the sense that if an upstream (T)NP port flaps again the problem will recur.

2 - Move the (T)NP ports to the end of the ports on the switch. For example, if there are four (T)NP uplinks on a MDS 9148 or MDS 9148S, then move them to fc1/45-fc1/48. Once this has been done the problem will not recur.

Related Documentation

The documentation set for NX-OS for the Cisco MDS 9000 Family includes the following documents. To find a document online, access the following web site:

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

The documentation set for Cisco Fabric Manager appears in the *Cisco Fabric Manager Release Notes for Release 4.2(1)*, which is available from the following website:

http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9500 Series Supervisor-2A Tech Note*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Licensing Guide*

- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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: www.cisco.com/go/trademarks. 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. (1110R)

© 2012 Cisco Systems, Inc. All rights reserved.

