Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.0(1a)

Release Date: February 22, 2010

Part Number: OL-21012-01 I0

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 43.

Note As of Cisco Fabric Manager Release 4.2(1a), Fabric Manager information will no longer appear in the Cisco MDS 9000 Family Release Notes for NX-OS releases. Cisco Fabric Manager Release Notes will include information that is exclusive to Fabric Manager as a management tool for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. Refer to the following website for Release Notes for Cisco Fabric Manager:
http://www.cisco.com/en/US/partner/products/ps10495/prod_release_notes_list.html

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   Online History Change

Revision	Date	Description
A0	02/22/2010	Created release notes.
B0	02/26/2010	• Added DDTS CSCte93219 as an Open Caveat. • Modified the description of DDTS CSCte93754.
C0	03/12/2010	• Modified the description of the "Support for FCIP Compression Modes" limitation. • Removed IVR Flows from the "I/O Accelerator Feature Limitations" section. • Added IOA with IVR and SME with IVR to the "New Features in Cisco MDS NX-OS Release 5.0(1a)" section.

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

Send documentation comments to mdsfeedback-doc@cisco.com

Table 1 **Online History Change**

Revision	Date	Description
D0	03/30/2010	• Added the "Determining Software Version Compatibility" section. • Addedthe "Discontinued Software Features" section.
E0	04/19/2010	• Added a note about the number of ITLs that can be configured when SME is deployed for IVR flows. See the "SME with IVR" section. • Clarified the information in the "Upgrading Effect on VSAN 4079" section. • Clarified the information about Fibre Channel ports in the "General Upgrading Guidelines" and the "General Downgrading Guidelines" sections.
F0	05/04/2010	• Added DDTS CSCsu96762.
G0	06/08/2010	• Added the "Features Not Supported on the Cisco MDS 9148 Switch" limitation.
H0	07/20/2010	• Modified the format and content of Table 7.
I0	07/27/2010	• Added the "PPRC Not Supported with FCIP Write Acceleration" limitation.

Contents

This document includes the following:

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** To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S2K9-5.0.1a	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-5.0.1a	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M91S2K9-5.0.1a	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9124 Switch and MDS 9134 Switch
	M91S3K9-5.0.1a	MDS 9148 Supervisor/Fabric-3 NX-OS software	MDS 9148 Switch
SSI Interface	SSI-M9K9-501a	Storage Services Interface for NX-OS Release 5.0(1a)	MDS 9000 Family
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

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

Component	Part Number	Description	Applicable Product
Licenses (continued)	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
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

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

Component	Part Number	Description	Applicable Product
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 Fabric1 Module	MDS 9513 Switch
	DS-13SLT-FAB2	Cisco MDS 9513 Switching Fabric2 Module	MDS 9513 Switch
Optics	DS-X2-FC10G-SR	X2 SC optics, 10-Gbps Fibre Channel for short reach	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-LR	X2 SC optics, 10-Gbps Fibre Channel for long reach (10 km)	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-ER	X2 SC optics, 10-Gbps Fibre Channel for extended reach (40 km)	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-CX4	X2 SC optics, 10-Gbps Fibre Channel over copper	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-E10G-SR	X2 SC optics, 10-Gbps Ethernet for short reach	MDS 9500 Series MDS 9200 Series

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

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP	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 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-FC-2G-SW	SFP optics (LC type) for 1- or 2-Gbps Fibre Channel for shortwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FC-2G-LW	SFP optics (LC type) for 1- or 2-Gbps Fibre Channel for longwave mode for Cisco MDS 9500, MDS 9200, and MDS 9100 Series; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	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
CD-ROM	M90FM-CD-441	Cisco MDS 9000 Management Software and Documentation CD-ROM for Cisco MDS 9000 NX-OS Software Release 4.1(3a)	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
MDS 9134	Yes
MD S 9124	Yes
Cisco Fabric Switch for HP c-Class BladeSystem and Cisco Fabric Switch for IBM BladeCenter	Yes

Note   A of Cisco MDS NX-OS Release 5.0(1a), support for the MDS 9216i switch is discontinued.

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.

Note   As of Cisco MDS NX-OS Release 5.0(1a), support for the following Generation 1 modules is discontinued:

- DS-X9302-14K9, 14/2-port Multiprotocol Services (MPS-14/2) Module
- DS-X9016, 16-port 1-, 2-Gbps Fibre Channel Switching Module
- DS-X9032, 32-port 1-, 2-Gbps Fibre Channel Switching Module
- DS-X9032SSM, 32-port Storage Services Module (SSM)

Generation 1 modules should be removed from a switch chassis before the installation of NX-OS Release 5.0(1a) begins.

Table 4   Module Support Matrix for Cisco MDS NX-OS 5.x

Module	Description	MDS 9500 Series	MDS 9222i
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A

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

Module	Description	MDS 9500 Series	MDS 9222i
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[1]	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[1]	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	Yes	Yes
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes

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

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

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-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[1]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[1]	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	Yes	Yes	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes

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

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	No	No	No
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	No	No	No

1. 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-SF1-K9	MDS 9500 Supervisor-1 Module	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A	N/A	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)[1]	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. Cisco SAN-OS Release 3.2(1) and later support the 18/4-Port Multiservice Module (MSM-18/4).

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

As of Cisco MDS SAN-OS Release 3.0(1), the Cisco MDS 9509 and 9506 Directors support both Supervisor-1 and Supervisor-2 modules. Supervisor-1 and Supervisor-2 modules cannot be installed in the same switch, except during migration. Both the active and standby supervisor modules must be of the same type, either Supervisor-1 or Supervisor-2 modules. For Cisco MDS 9513 Directors, both supervisor modules must be Supervisor-2 modules.

⚠️ **Caution**   Migrating your supervisor modules is a disruptive operation.

✎ **Note**   Migrating from Supervisor-2 modules to Supervisor-1 modules is not supported.

To migrate from a Supervisor-1 module to a Supervisor-2 module, refer to the step-by-step instructions in the *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide.*

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 13
- Selecting the Correct Software Image for an MDS 9100 Series Switch, page 14
- Selecting the Correct Software Image for an MDS 9200 Series Switch, page 14
- Selecting the Correct Software Image for an MDS 9500 Series Switch, page 14

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 the Fabric Manager, 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

NX-OS Software	Minimum NX-OS Release	Tested NX-OS Release
NX-OS Release 5.0(1a)	SAN-OS Release 3.3(1c) or later	SAN-OS Release 3.3(1c), 3.3(4a)
	NX-OS Release 4.1(1b) or later	NX-OS Releases 4.1(1b), 4.2(3)

Fabric Manager Software	Minimum NX-OS Release	Tested NX-OS Releases
Fabric Manager Release 5.0(1a)	SAN-OS Release 3.3(1c) or later	NX-OS Release 3.3(1c), 3.3(4a)
	NX-OS Release 4.1(1b) or later	NX-OS Release 4.1(1b), 4.2(3)
	NX-OS Release 5.0(1a) or later	NX-OS Release 5.0(1a)

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/public/sw-center

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 Fabric Manager 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, 9124, Cisco Fabric Switch for HP c-Class BladeSystem, Cisco Fabric Switch for IBM BladeCenter	Filename begins with m9100-s2ek9
MDS 9148	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	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
```

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:

- General Upgrading Guidelines, page 15
- Upgrading Effect on VSAN 4079, page 19
- FICON Supported Releases and Upgrade Paths, page 18
- Upgrading with IVR Enabled, page 19
- Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch, page 20
- Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch, page 20
- Performing a Disruptive Upgrade on an MDS 9000 Family Switch, page 20
- Resetting SNMP Notifications, page 21

Note Before you begin the upgrade process, review the list of chassis and modules that Cisco MDS NX-OS Release 5.0(1a) supports. See the "MDS 9000 Chassis and Module Support" section on page 9.

For detailed instructions for performing a software upgrade using Cisco Fabric Manager, see the *Cisco Fabric Manager Release Notes for Release 4.2(1a)*, which is available from the following website:

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

General Upgrading Guidelines

Note To upgrade to NX-OS Release 5.0(1a) from SAN-OS Release 3.2(3a) or earlier, first upgrade to SAN-OS Release 3.3(x), then upgrade to NX-OS Release 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a).

Use the following guidelines when upgrading to Cisco MDS NX-OS Release 5.0(1a):

- Install and configure dual supervisor modules.
- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- Follow the recommended guidelines for upgrading a Cisco MDS 9124 or MDS 9134 Switch as described in "Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch" section on page 20.
- Follow the guidelines for upgrading a single supervisor switch as described in "Performing a Disruptive Upgrade on an MDS 9000 Family Switch" section on page 20.
- Be aware of the impact of an upgrade on VSAN 4079 if you are upgrading from SAN-OS Release 3.x to NX-OS 5.0(1a). See the "Upgrading Effect on VSAN 4079" section on page 19 for details.
- 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.

- **SSM**: Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.

- **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 MPS-14/2 module, 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.

- **Inter-VSAN Routing (IVR)**: With IVR enabled, you must follow additional steps if you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the "Upgrading with IVR Enabled" section on page 19 for these instructions.

- **FICON**: If you have FICON enabled, the upgrade path is different. See the "FICON Supported Releases and Upgrade Paths" section on page 18.

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.

Use Table 11 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 5.0(1a), find the image release number you are currently using in the Current column of the table, and use the path recommended.

Note The software upgrade information in Table 11 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

Table 11   Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 5.0(1a)

Current Release	Nondisruptive Upgrade Path
NX-OS:	
4.2(3) 4.2(1b) 4.2(1a) 4.1(3a) 4.1(1c) 4.1(1b)	You can nondisruptively upgrade directly to NX-OS Release 5.0(1a)
SAN-OS:	
3.3(4) 3.3(3) 3.3(2) 3.3(1c) 3.3(1a)	Upgrade to NX-OS 4.1(x) or 4.2(x) and then upgrade to NX-OS Release 5.0(1a).
3.2(3a) 3.2(3) 3.2(2c) 3.2(1a) 3.1(4) 3.1(3a) 3.1(2b) 3.1(2a) 3.1(2) 3.1(1) 3.0(3a) 3.0(3) 3.0(2a) 3.0(2) 3.0(1) 2.1(3) 2.1(2e) 2.1(2d) 2.1(2b)	Upgrade to SAN-OS Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a).
2.1(2) 2.1(1b) 2.1(1a) 2.0(x)	Upgrade to SAN-OS Release 2.1(2b), then upgrade to Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a) or Upgrade to SAN-OS Release 2.1(2d), then upgrade to Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a) or Upgrade to SAN-OS Release 2.1(2e), then upgrade to Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a) or Upgrade to SAN-OS Release 2.1(3), then upgrade to Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a)
1.x	Upgrade to SAN-OS Release 1.3(4a), then upgrade to Release 2.1(2b), then upgrade to Release 3.3(x), then upgrade to NX-OS 4.1(x) or 4.2(x), and then upgrade to NX-OS Release 5.0(1a).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 5.0(1a) does not support FICON

Table 12 lists the SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

Table 12   FICON Supported Releases

FICON Supported Releases	
NX-OS	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 your FICON nondisruptive upgrade path to Cisco MDS NX-OS Release 5.0 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 to MDS NX-OS Release 4.2(1b)

Current Release with FICON Enabled	Upgrade Path
NX-OS 4.1(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS 3.3(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS 3.2(2c)	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).
SAN-OS 3.0(3b)	
SAN-OS 3.0(3)	
SAN-OS 3.0(2)	
SAN-OS 2.0(2b)	Use the **interface shutdown** command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively upgrading from SAN-OS Release 2.0(2b) to SAN-OS Release 3.0(2) or SAN-OS Release 3.0(3b), and then upgrade to Release 3.3(1c). An operationally down state includes `Link failure or not-connected`, `SFP not present`, or `Error Disabled` status in the output of a **show interface** command. When an interface is administratively shut it will then show as `Administratively down`. Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.x	Upgrade to SAN-OS Release 3.0(2). Use the **interface shutdown** command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively upgrading to Release 2.0(2b) and then upgrade to 1.3(4a).

Upgrading Effect on VSAN 4079

If you upgrade to NX-OS Release 5.0(1a), and you have not created VSAN 4079, the NX-OS software will automatically create VSAN 4079 and reserve it for EVFP use.

If VSAN 4079 is reserved for EVFP use, the **switchport trunk allowed vsan** command will filter out VSAN 4079 from the allowed list. In the following example, the allowed list appears on a separate line following the command:

```
switch(config-if)# switchport trunk allowed vsan 1-4080
1-4078,4080
switch(config-if)#
```

If you have created VSAN 4079, the upgrade to NX-OS Release 5.0(1a) will have no affect on VSAN 4079.

If you downgrade to a release of NX-OS lower than NX-OS Release 4.1(x) after NX-OS Release 5.0(1a) creates VSAN 4079 and reserves it for EVFP use, the VSAN will no longer be reserved.

Upgrading with IVR Enabled

An Inter-Switch Link (ISL) flap resulting in fabric segmentation or a merge during or after an upgrade from Cisco MDS SAN-OS Release 2.0(x) to a later image where IVR is enabled might be disruptive. Some possible scenarios include the following:

- FCIP connection flapping during the upgrade process resulting in fabric segmentation or merge.
- ISL flap results in fabric segmentation or merge because of hardware issues or a software bug.
- ISL port becomes part of PCP results in fabric segmentation or merge because of a port flap.

If this problem occurs, syslogs indicate a failure and the flapped ISL could remain in a down state because of a domain overlap.

This issue was resolved in Cisco SAN-OS Release 2.1(2b); you must upgrade to Release 2.1(2b) before upgrading to Release 3.3(1c). An upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) when IVR is enabled requires that you follow the procedure below. If you have VSANs in interop mode 2 or 3, you must issue an IVR refresh for those VSANs.

To upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) for all other VSANs with IVR enabled, follow these steps:

Step 1 Configure static domains for all switches in all VSANs where IVR is enabled. Configure the static domain the same as the running domain so that there is no change in domain IDs. Make sure that all domains are unique across all of the IVR VSANs. We recommend this step as a best practice for IVR-non-NAT mode. Issue the **fcdomain domain** *id* **static vsan** *vsan id* command to configure the static domains.

> **Note** Complete Step 1 for all switches before moving to Step 2.

Step 2 Issue the **no ivr virtual-fcdomain-add vsan-ranges** *vsan-range* command to disable RDI mode on all IVR enabled switches. The range of values for a VSAN ID is 1 to 4093. This can cause traffic disruption.

> **Note** Complete Step 2 for all IVR enabled switches before moving to Step 3.

Step 3 Check the syslogs for any ISL that was isolated.

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
PortChannel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface PortChannel 51
(reason: domain ID assignment failure)
```

Step 4 Issue the following commands for the isolated switches in Step 3:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan vsan-id suspend
switch(config-vsan-db)# no vsan vsan-id suspend
```

Step 5 Issue the **ivr refresh** command to perform an IVR refresh on all the IVR enabled switches.

Step 6 Issue the **copy running-config startup-config** command to save the RDI mode in the startup configuration on all of the switches.

Step 7 Follow the normal upgrade guidelines for Release 2.1(2b). If you are adding new switches running Cisco MDS SAN-OS Release 2.1(2b) or later, upgrade all of your existing switches to Cisco SAN-OS Release 2.1(2b) as described in this workaround. Then follow the normal upgrade guidelines for Release 3.3(1c).

> **Note** RDI mode should not be disabled for VSANs running in interop mode 2 or interop mode 3.

Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch

If you are upgrading from Cisco MDS SAN-OS Release 3.1(1) to Cisco NX-OS Release 4.2(1b) before upgrading to NX-OS Release 5.0(1a) on a Cisco MDS 9124 or MDS 9134 Switch, follow these guidelines:

- During the upgrade, configuration is not allowed and the fabric is expected to be stable.
- The Fabric Shortest Path First (FSPF) timers must be configured to the default value of 20 seconds; otherwise, the nondisruptive upgrade is blocked to ensure that the maximum down time for the control plane can be 80 seconds.
- If there are any CFS commits in the fabric, the nondisruptive upgrade will fail.
- If there is a zone server merge in progress in the fabric, the nondisruptive upgrade will fail.
- If a service terminates the nondisruptive upgrade, the **show install all failure-reason** command can display the reason that the nondisruptive upgrade cannot proceed.
- If there is not enough memory in the system to load the new images, the upgrade will be made disruptive due to insufficient resources and the user will be notified in the compatibility table.

Performing a Disruptive Upgrade on an MDS 9000 Family Switch

If you do not follow the upgrade path when performing a disruptive upgrade on an MDS 9000 Family switch, (for example, you upgrade directly from SAN-OS Release 2.1(2) or earlier version to NX-OS Release 4.2(x)), the binary startup configuration is deleted because it is not compatible with the new

image, and the ASCII startup configuration file is applied when the switch comes up with the new upgraded image. When the ASCII startup configuration file is applied, there may be errors. Because of this, we recommend that you follow the nondisruptive upgrade path.

> **Note** You cannot upgrade the software image on an MDS 9120 switch, an MDS 9140 switch, or an MDS 9216i switch to Cisco NX-OS Release 5.x. See Table 3 for the list of switches that support Cisco NX-OS Release 5.0(1a).

Resetting SNMP Notifications

Following a software upgrade or downgrade, SNMP notifications will reset as follows:

- When you upgrade from SAN-OS Release 3.x to NX-OS Release 4.1(x), and then to NX-OS Release 5.x, SNMP notifications will reset to their default settings.
- When you upgrade from SAN-OS Release 3.x to NX-OS Release 4.2(x), and then to NX-OS Release 5.x, SNMP notifications will not reset to their default settings.
- When you downgrade from any NX-OS Release 4.2(x), SNMP notifications will reset to their default configuration settings.

Use the **snmp-server enable traps** command to reenable your required SNMP notifications.

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:

- General Downgrading Guidelines, page 21
- New Features in Cisco MDS NX-OS Release 5.0(1a), page 24

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS NX-OS Release 5.0(1a):

- Install and configure dual supervisor modules.
- 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:
  - **Fibre Channel Ports**: Fibre Channel ports can be nondisruptively downgraded without affecting traffic on the ports. See Table 14 for the nondisruptive downgrade path for all SAN-OS releases.

- **SSM**: Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during a downgrade. SSM Fibre Channel traffic is not.

- **Gigabit Ethernet Ports**: Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, 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.

- **IVR**: With IVR enabled, you must follow additional steps if you are downgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the "Upgrading with IVR Enabled" section on page 19 for these instructions.

- **FICON**: If you have FICON enabled, the downgrade path is different. See the "FICON Downgrade Paths" section on page 24.

Note A downgrade from NX-OS Release 4.2(1b) to SAN-OS Release 3.3(1x) is not supported on MDS switches, when FC-Redirect based applications, such as Data Mobility Manager or Storage Media Encryption, are configured in the fabric if either of the following conditions are satisfied:

1. A target for which FC-Redirect is configured is connected locally and there are Generation 1 modules with ISLs configured in the switch.

2. A host, for which FC-redirect is configured, is connected locally on a Generation 1 module.

If these conditions exist, remove the application configuration for these targets and hosts before proceeding with the downgrade.

Use Table 14 to determine the nondisruptive downgrade path from Cisco NX-OS Release 4.2(1b). Find the SAN-OS image you want to downgrade to in the To SAN-OS Release column of the table and use the path recommended.

Note The software downgrade information in Table 14 applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

Table 14   Nondisruptive Downgrade Path from NX-OS Release 5.0(1a)

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path
NX-OS:	
4.2(3) 4.2(1b) 4.2(1a) 4.1(3a) 4.1(1c) 4.1(1b)	You can nondisruptively downgrade directly from NX-OS Release 5.0(1a).
SAN-OS:	
3.3(4) 3.3(3) 3.3(2) 3.3(1c) 3.3(1a)	Downgrade to NX-OS Release 4.2(x) or Release 4.1(x) first, and then downgrade to SAN-OS Release 3.3(x).
3.2(3a) 3.2(3) 3.2(2c) 3.2(1a) 3.2(1) 3.1(4) 3.1(3a) 3.1(3) 3.1(2b) 3.1(2a) 3.1(2) 3.0(3a) 3.0(3) 3.0(2a) 3.0(2) 3.0(1) 2.1(3) 2.1(2e) 2.1(2d) 2.1(2b) 2.1(2) 2.1(2b) 2.1(1a)	Downgrade to NX-OS Release 4.2(x) or Release 4.1(x) first, then downgrade to SAN-OS Release 3.3(x), and then downgrade to Release 3.2(x), Release 3.1(x)., Release 3.0(x), or Release 2.1(x).
2.0(4a) 2.0(4) 2.0(3) 2.0(2b) 2.0(1b)	Downgrade to NX-OS Release 4.2(x) or Release 4.1(x) first, then downgrade to SAN-OS Release 3.3(x), then downgrade to Release 2.1(2x), and then downgrade to Release 2.0(x).
1.x	Downgrade to NX-OS Release 4.2(x) or Release 4.1(x) first, then downgrade to SAN-OS Release 3.3(x), then downgrade to SAN-OS to Release 2.1(2b), then to Release 1.3(4a), and then downgrade to your SAN-OS 1.x release.

FICON Downgrade Paths

Table 15 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 15   FICON Downgrade Path from NX-OS Release 4.1(1c)

To Release with FICON Enabled	Downgrade Path
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).
SAN-OS 2.0(2b)	Use the **interface shutdown** command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively downgrading from NX-OS Release 4.1 to SAN-OS Release 3.3(1c) then to SAN-OS Release 3.0(3b) or SAN-OS Release 3.0(2), and then to SAN-OS Release 2.0(2b). An operationally down state includes `Link failure or not-connected`, `SFP not present`, or `Error Disabled` status in the output of a **show interface** command. When an interface is administratively shut it will then show as `Administratively down`. Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.3(4a)	Downgrade to SAN-OS Release 3.3(1c) and then to Release 3.0(2). Use the shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively downgrading to Release 2.0(2b) and then downgrade to 1.3(4a).

New Features in Cisco MDS NX-OS Release 5.0(1a)

Cisco NX-OS Release 5.0(1a) is a software release that includes new features, enhancements, and bug fixes. It also supports the launch of the new MDS 9148 Multilayer Fabric Switch.

This release includes the following major features:

- Secure Erase on the MSM-18/4 and the MDS-9222i
- AAA Enhancements
- IOA with IVR
- SME with IVR
- SFP Diagnostics

For descriptions of the new features in Fabric Manager Release 5.0(1a), see the *Cisco Fabric Manager Release Notes for Release 5.0(1a).*

NX-OS Feature Descriptions

This section includes descriptions of the major new features of MDS NX-OS Release 5.0(1a) and indicates where the feature is documented.

Secure Erase on the MSM-18/4 and the MDS 9222i

Cisco Secure Erase for the Cisco MDS 9500 or MDS 9200 family of switches provides significant advantages over traditional data erase mechanisms. These advantages include platform independence, higher speed, lower cost, and easier deployment. Cisco Secure Erase uses special algorithms to erase data. These algorithms erase data by specifying pattern sequences that are repeatedly written to the target media. This process overcomes the traditional problem of data remnants. The Secure Erase feature runs on the intelligent module, which is responsible for managing the data erasing process. The host or servers connected to the SAN have no role in the data erasing process. The storage ports can be connected anywhere in the SAN provided they are accessible from the switch where Cisco Secure Erase is running. Cisco Secure Erase supports 6 algorithms, 2 of the algorithms are Department of Defense approved, one is approved by Royal Canadian Mounted police and the remaining three are commercial algorithms.

Where Documented

For documentation on the Cisco Secure Erase feature, see the *Cisco MDS 9000 Secure Erase Configuration Guide.*

AAA Enhancements

Starting inCisco NX-OS Release 5.0(1a), NX-OS supports LDAP and Active Directory for AAA authentication at the command-line interface (CLI) level.

Where Documented

For documentation on AAA Enhancements, see the *Cisco MDS 9000 Family NX-OS Security Configuration Guide* and the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide.*

IOA with IVR

Starting in Cisco NX-OS Release 5.0(1a), IOA supports IVR flows and can operate seemlessly in IVR environments.

Where Documented

For documentation on IOA with IVR, see the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide* and the *Cisco MDS 9000 I/O Accelerator Configuration Guide.*

SME with IVR

Cisco Storage Media Encryption (SME) supports IVR as of Cisco NX-OS Release 5.0(1a).

> **Note** When SME is deployed with IVR flows, the number of Initiator Target LUNs (ITLs) that can be configured is 512. This limit is different than the published limit in the *Cisco SME Configuration Limits* section of the *Cisco MDS 9000 Family Storage Media Encryption Guide*.

Where Documented

For documentation on SME with IVR, see the *Cisco MDS 9000 Family Storage Media Encryption Guide.*

SFP Diagnostics

Any error message related to SFP failures or SNMP traps will be written to syslog. Customers can listen to syslog for events related to SFP failures.

Where Documented

For documentation on SFP messages that are written to syslog, see the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide.*

Discontinued Software Features

As of NX-OS Release 5.0(1a), support for Fabric Congestion Control (FCC) is discontinued. If you are currently using FCC in your SAN environment, you should turn it off before upgrading to NX-OS Release 5.0(1a). Use the **no fcc enable** command to turn off the FCC feature.

Hardware Changes

This section describes hardware changes associated with NX-OS Release 5.0(1a).

MDS 9148 Multilayer Fabric Switch

The Cisco MDS 9148 Multilayer Fabric Switch is a high-performance, flexible, cost-effective platform that provides high-density, line-rate 8-Gbps ports for storage networking deployments in small, medium-sized, and large enterprise environments. The MDS 9148 offers up to 48 autosensing Fibre Channel ports capable of speeds of 1-, 2-, 4-, or 8-Gbps. The switch comes with three preconfigured models for 16, 32, or 48 ports. The 16- and 32-ports models can be upgraded onsite to enable additional ports by adding one or more 8-port Cisco MDS 9148 On-Demand Port Activation licenses.

Where Documented

For hardware installation information about the MDS 9148 switch, see the *Cisco MDS 9100 Series Hardware Installation Guide.* For software information related to the MDS 9148 switch, see the *Cisco MDS 9000 NX-OS Interfaces Configuration Guide* and the *Cisco MDS 9000 Family Command Reference.*

Generation 1 Hardware Support Discontinued

Cisco MDS NX-OS Release 5.0(1a) does not support the following Generation 1 modules:

- DS-X9302-14K9 - 14/2-port Multiprotocol Services (MPS-14/2) Module

- DS-X9016 - 16-port 1-, 2-Gbps Fibre Channel Switching Module
- DS-X9032 - 32-port 1-, 2-Gbps Fibre Channel Switching Module
- DS-X9032SSM - 32-port Storage Services Module (SSM)

Generation 1 modules should be removed from a switch chassis before the installation of NX-OS Release 5.0(1a) begins.

In addition, Cisco MDS NX-OS Release 5.0(1a) does not support the MDS 9216i switch.

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, Fabric Manager Server (FMS) 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.

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 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. XRC acceleration is not supported on the SSN-16.

Limitations and Restrictions

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

Support for Generation One Modules

As of Cisco MDS NX-OS Release 5.0(1a), support for Generation One modules has been discontinued. See the "Support for Generation One Modules" section for more information.

IPv6

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

User Roles

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

- In a network environment, users often need to view information in other VSANs even though they do not have permission to modify configurations in those VSANs.
- This behavior makes Cisco MDS 9000 Series switches consistent with other Cisco products, such as Cisco Nexus 7000 Series switches, that exhibit the same behavior for those roles (when they apply to the VLAN policy).

Red Hat Enterprise Linux

The Linux kernel core dump is not supported in NX-OS Release 4.1(1b) and later versions and therefore the CLI command has been removed. A syntax error message will be displayed if you import configurations from SAN-OS Release 3.3(x) and earlier to NX-OS Release 4.1(1b) and later. These

syntax errors do not affect the application of other commands in the configuration and can be safely ignored. To address this, remove the kernel core configuration from the ASCII configuration file before importing the configuration.

Generation 1 Module Limitation

When a Cisco or other vendor switch port is connected to a Generation 1 module port (ISL connection), the receive buffer-to-buffer credit of the port connected to a Generation 1 module port should not exceed 255.

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 xyxxyx
```

Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.0(1a)

```
>    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.

- VSAN 4079 will be impacted by an upgrade to NX-OS Release 4.1(3a), depending on whether or not VSAN 4079 was created prior to the upgrade. See the "Upgrading Effect on VSAN 4079" section on page 19 for details.

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:

- Devices with NPV and NPIV enabled
- F port trunking
- F port channeling

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:

- IVR
- 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.

Caveats

This section lists the open and resolved caveats for this release. Use Table 16 to determine the status of a particular caveat. In the table, "O" indicates an open caveat and "R" indicates a resolved caveat.

Table 16   Open Caveats and Resolved Caveats Reference

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.2(3)	5.0(1a)
Severity 2		
CSCsz53741	O	R
CSCsz59152	O	R
CSCsz84411	O	R
CSCtb74201	O	R
CSCtd77695	O	R
CSCtd47883	O	R
CSCtd48744	O	R
CSCtd59553	O	R
CSCtd90345	O	R
CSCte37124	O	R
CSCte93754	–	O
CSCtf16263	–	O
Severity 3		
CSCsq20408	O	O
CSCsy37951	O	O
CSCsz16768	O	R
CSCta62636	O	R
CSCtc03274	O	R
CSCtc33466	O	R

Table 16 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.2(3)	5.0(1a)
CSCtc62666	O	R
CSCtc68983	O	R
CSCtd34299	O	R
CSCtd59561	O	R
CSCtd66543	O	R
CSCtd78318	O	R
CSCtd96328	O	R
CSCte27874	O	R
CSCte93219	–	O
Severity 4		
CSCtc65441	O	R
CSCtc68140	O	R
CSCte46571	O	R
Severity 5		
CSCtd55394	O	R
Severity 6		
CSCsu96762	O	R
CSCsz01436	O	R
CSCte42184	O	R

Resolved Caveats

- CSCsz53741

  Symptom: When a crossbar module fails due to sync loss, MDS switches try to recover the fabric module by power cycling the crossbar. This may result in lost data path connectivity because the recovery may not complete.

  Workaround: This issue is resolved.

- CSCsz59152

  Symptom: When a crossbar module fails due to sync loss, MDS switches try to recover the fabric module by power cycling the crossbar. This may result in lost data path connectivity because the recovery may not complete.

  Workaround: This issue is resolved.

- CSCsz84411

  Symptom: An MDS 9124 switch may randomly reboot with a reset reason of unknown. This is a rare event and occurs only in systems that have a single power supply with a serial number beginning with QCS.

Workaround: This issue is resolved.

- CSCtb74201

  Symptom: When stale, non-advertised IVR virtual domain entries get stuck in persistent storage service (PSS) after an HA failover, upgrading the switch with these stale entries to SAN-OS Release 3.3(2) or later may fail to clear up these entries because of some corner cases where an unexpected location of the PSS cursor occurs. This in turn may lead to IVR zone set activation failures.

  Workaround: This issue is resolved.

- CSCtd77695

  Symptom: When a tape reaches its capacity, IBM TS1120 tape drives send a check condition with eom = 1 and asc_ascq = 0. Because asc_ascq is not set to End of Medium or Partition, SME continues to send traffic as if the end of tape is not reached. This situation causes the backup to fail when it spans across multiple tapes. This problem is specific to IBM TS1120 tape drives.

  Workaround: This issue is resolved.

- CSCtd47883

  Symptom: In certain rare circumstances, when the IOA cluster membership across the switches flaps due to a switchover or loss of connectivity to the management interface, certain internal control messages get dropped, which causes the flows to stay in a stuck state.

  Workaround: This issue is resolved.

- CSCtd48744

  Symptom: On an MDS 9222i switch, when IVR is enabled in non-NAT mode and the in-order-guarantee feature is enabled, a route change, such as an ISL going up or down, can cause an exception similar to the following on Generation 2 or Generation 3 modules:

```
********* Exception info for module 1 ********

exception information --- exception instance 1 ----
Module Slot Number: 1
Device Id       : 54
Device Name     : Tuscany-xbar
Device Errorcode  : 0xc3600107
Device ID       : 54 (0x36)
Device Instance  : 00 (0x00)
Dev Type (HW/SW)  : 01 (0x01)
ErrNum (devInfo)  : 07 (0x07)
System Errorcode  : 0x40420031 Tuscany xbar module experienced an error
Error Type       : Minor error
PhyPortLayer     : Fibre Channel Virtual
Port(s) Affected  : 19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34
Error Description :
DSAP             : 0 (0x0)
UUID             : 0 (0x0)
Time             : Mon Nov 16 10:07:33 2009
                    (Ticks: 4B012465 jiffies)

exception information --- exception instance 2 ----
Module Slot Number: 1
Device Id       : 54
Device Name     : Tuscany-xbar
Device Errorcode  : 0xc3600107
Device ID       : 54 (0x36)
Device Instance  : 00 (0x00)
Dev Type (HW/SW)  : 01 (0x01)
ErrNum (devInfo)  : 07 (0x07)
System Errorcode  : 0x40420031 Tuscany xbar module experienced an error
```

```
Error Type        : Minor error
PhyPortLayer      : Fibre Channel
Port(s) Affected  : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Error Description :
DSAP              : 0 (0x0)
UUID              : 0 (0x0)
Time              : Mon Nov 16 10:07:33 2009
                       (Ticks: 4B012465 jiffies)
```

All FC and FCIP interfaces go into a hardware failure state and the switch needs to be reloaded to recover. This error occurs only if in-order-delivery is enabled on one or more VSANs carried over an FCIP trunk.

Workaround: This issue is resolved.

- CSCtd59553

  Symptom: A PortChannel member change can result in route or IVR rewrite corruption or both if the following conditions are met:

  – In-order delivery (IOD) is enabled on the switch or in the fabric

  – More than one Equal Cost Multipath (ECMP) made of PortChannels is present.

  Workaround: This issue is resolved.

- CSCtd90345

  Symptom: Hosts running Tivoli Storage Manager (TSM) may experience read/write errors when IOA tape acceleration is enabled. This situation occurs because TSM always sends UNTAGGED commands and IOA sends its own commands such as READ, SPACE6, REWIND, etc. for read acceleration as TAGGED commands. When there is a mixture of UNTAGGED and TAGGED commands, an overlapping occurs because of out-of-order commands, which causes the tape drive to send a reject message.

  Workaround: This issue is resolved.

- CSCte37124

  Symptom: RSCNs are not sent out to the affected devices when the enhanced device alias members present in the active zone set are changed.

  Workaround: This issue is resolved.

- CSCsz16768

  Symptom: When NPV is enabled, IP access list commands are not available.

  Workaround: This issue is resolved.

- CSCta62636

  Symptom: Prior to MDS NX-OS Release 5.0(1a), MDS 9500 Series switches shipped with an Apache HTTP server. Some versions of the Apache web server enable HTTP Trace and Track methods on the switch, which exposes an XST vulnerability. See http://www.kb.cert.org/vuls/id/867593 for additional information.

  Workaround: This issue is resolved. The Apache server has been replaced by the THTTPD server that does not exhibit this vulnerability.

- CSCtc03274

Symptom: The zone server fails the zone check for the host and virtual target with iSAPI, and then rejects the host's PLOGI request. This happens because of the two-second delay between the PLOGI sent from host to the target, and because of the host port online RSCN. The issue also happens when a host goes down and comes back after a zone set activation.This issue only occurs when hosts are connected to a McData switch.

Workaround: This issue is resolved.

- CSCtc33466

    Symptom: Following a successful IVR zone merge between two Cisco MDS fabrics, where each fabric already had an active local IVR VSAN topology with an active IVR zone set, a new active zone set with a concatenated IVR zone set was created, as well as two IVR zone sets in the full zone set. However, when the **ivr copy active-zoneset full-zoneset** command was entered, the full IVR zone set was not overwritten.

    This symptom can occur if the zone ID or zone name of active zone set database and full zone set database are the same. In such cases, the copy operation will not occur.

    Workaround: This issue is resolved.

- CSCtc62666

    Symptom: Write operations to the bootflash: file system on an MDS 9124 switch fail because the bootflash: file system is read only. This issue only occurs on MDS 9124 systems released in 2009.

    You can confirm this issue as follows:

    - Check the console bootup logs for the following message:

    ```
      Checking all filesystems....r.ERROR: bootflash: has unrecoverable error; please do
    "format bootflash:"
    ```

    - Check for syslog messages such as:

    ```
      %KERN-2-SYSTEM_MSG: EXT3-fs error (device hda4): ext3_readdir: bad entry in
    directory #11:
      rec_len %% 4 != 0 - offset=0, inode=4294967295, rec_len=65535, name_len=255 - kernel

      %KERN-2-SYSTEM_MSG: Remounting filesystem read-only -kernel
    ```

    - When you try to write to the bootflash: file system, look for errors such as:

    ```
    switch# copy tftp://1.2.3.4/testfile bootflash:
      /bin/copy: cannot create regular file `/bootflash/testfile': Read-only file system.
    ```

    Workaround: This issue is resolved.

- CSCtc68983

    Symptom: Following an upgrade from SAN-OS Release 3.0(2a) to Release 3.3(2) on a switch with IVR1 in non-NAT mode, IVR zone set activation does not go through successfully. An error message like the following was displayed:

    ```
    2009 Oct  9 18:23:56 <switchname> %IVR-2-CFS_PEER_LOST_WITHIN_SESSION: CFS peer with
    switch wwn 20:00:00:0d:ec:27:92:c0 was lost in the middle of an active CFS session.
    Abort the CFS session and re-enter the configuration changes
    ```

    The IVR_DU database had a missing entry for the device which caused it to be stuck in advertising state.

    Workaround: This issue is resolved.

- CSCtd34299

Symptom: If you enter the **show dmm tech-support** command after a DMM Job fails, DMM cores and the module reloads.

Workaround: This issue is resolved.

- CSCtd59561

Symptom: SME hosts are unable to see the tape drives presented to them.

Workaround: This issue is resolved.

- CSCtd66543

Symptom: A memory leak in the Fabric-Device Management Interface (FDMI) process occurs whenever a port to which the FDMI host is connected is flapped. If there are many port flaps, the FDMI process may run out of memory and fail because memory is lost each time a port goes down.

Workaround: This issue is resolved.

- CSCtd78318

Symptom: Incorrect counting of zone members prevents the active zone database from being copied to the full zone database.

This situation occurs when you attempt copy a zone database (active or backup) to the full zone database. This action creates a new session, and the session database has as many members as the number of members in the active (or backup) database. The session is not counting unique members in the zone database. Instead it is counting repeated members (across different zones) as separate members. Because of the repeated members, the number of zone members in the zoning database exceeds 20,000, which is the maximum supported number of members.

Workaround: This issue is resolved.

- CSCtd96328

Symptom: The **no system health module** *slot* **loopback failure-action** command does not work as expected. When an interface goes into hardware failure state because of congestion on the port, this command should help the interface not go into a hardware failure state, but it does not.

Workaround: This issue is resolved.

- CSCte27874

Symptom: An MDS switch shows high CPU usage when viewed in Device Manager. If you enter the **show process cpu** command, the output shows the following:

```
PID    Runtime(ms)      Invoked   uSecs       1Sec    Process
-----  ---------------  --------  ---------   -----   -----------
1675   2215685686       268836864 1565842753  94.3    vrrp-eng
```

The virtual router redundancy protocol (VRRP) engine is using more than 90% of the available CPU time. This situation is caused by improper handling of VRRP-HA (authentication header) packets on the supervisor.

Workaround: This issue is resolved.

- CSCtc65441

Symptom: When excessive traffic or errors occur on the mgmt0 port, an MDS 9124 switch may fail and reload because of a watchdog timeout error.

Workaround: This issue is resolved.

- CSCtc68140

Symptom: An IVR switch was stuck in the advertising state shortly after a zone set activation was received by IVR. The zone set activation was complete, but IVR remained stuck in the advertising state.

Workaround: This issue is resolved.

- CSCte46571

Symptom: The **show cores** command displays the timestamp of the core files, but does not include the year.

Workaround: This issue is resolved.

- CSCtd55394

Symptom: If the ES or NS storage LUNs that are part of DMM are reconfigured when a DMM job is running on these LUNs, the DMM job will fail because the storage array (either ES or NS) returns CHECK CONDITION ASCQ 0x3F.

Workaround: This issue is resolved.

- CSCsu96762

Symptom: The crossbar links between an MDS fibre channel switching module and a fabric module are high-speed serials links, and on rare occasions, they can get out of sync. Because of this, a mechanism is in place in the NX-OS software to recover from sync loss. If the sync loss recovery is successful, the module that had the sync loss stays up. In the event of crossbar sync loss, there is packet loss. In extremely rare situations, it is possible to have a continuous sequence of sync loss followed by sync loss recovery.

Workaround: This issue is resolved. A crossbar manager has been added to NX-OS Release 5.0(1a) that does the following:

1. Reloads the switching module if there are numerous recoverable sync losses within a given time period.

2. Reloads the switching module up to three times if the recoverable sync loss persists.

3. Powers down the switching module if the failure continues to persist.

- CSCsz01436

Symptom: The **snmp-server system-shutdown** command is on by default and cannot be disabled.

Workaround: This issue is resolved.

- CSCte42184

Symptom: SAN extension ports on the fixed slot of a MDS 9222i switch do not require a license. However, the fact that a license is not required is not clear from the output of the **show license usage** command.

Workaround: This issue is resolved. The output of the **show license** command has been modified to explicitly show that the SAN extension license for the base switch is included.

Open Caveats

- CSCte93754

Symptom: An IOA flow can take a few seconds to become active in certain events such as host or target port flaps. PLOGIs from the hosts are buffered until the IOA flow becomes active. Once the IOA flow becomes active, a RSCN is sent, which forces the host to perform a PLOGI again. Certain target arrays perform a few back-to-back PLOGIs prior to the flow becoming active, which may cause automatic path recovery to fail.

Workaround: To prevent exhausting PLOGI retries, set the wa-fcr-rule timeout to 5 seconds through the CLI. Enter the **tune wa-fcr-rule-timeout 5** command in the IOA cluster.

- CSCtf16263

    Symptom: Following an upgrade from Cisco MDS NX-OS Release 4.2(3a) to Release 5.0(1a) on an MDS 9222i switch, the Encapsulating Security Protocol (ESP) configuration is not applied to members of a PortChannel. This issue occurs only on the MDS 9222i switch.

    Workaround: To workaround this issue, following these steps:

1. Enable Fibre Channel Security Protocol (FCSP) on the interface and enter configuration-interface-esp submode.

    ```
    switch(config)# interface po103
    switch(config-if)# fcsp on
    switch(config-if)# fcsp esp manual
    ```

2. Add the old egress Security Association (egress-sa) configuration on the switch. Egress-sa is the other side of the active ingress-sa.

    ```
    switch(config-if-esp)# egress-sa 258
    ```

3. Add a new ingress-sa on the switch. Do not use the previous SA.

    ```
    switch(config-if-esp)# ingress-sa 256
    ```

4. On the other side of the PortChannel, reconfigure egress with 256.

    ```
    switch(config)# interface po103
    switch(config-if)# fcsp esp manual
    switch(config-if-esp)# egress-sa 256
    ```

    At this point, the link is fully secured on both sides.

5. Clean up the old ingress-sa, by deleting it. An error message displays, but the ingress-sa does get deleted.

    ```
    switch(config-if-esp)# no ingress-sa 258
    ERROR: SA 258 not in ingress list
    ```

    If you fail to delete the old ingress-sa, an error message displays:

    ```
    switch(config-if-esp)# ingress-sa 258
    ERROR: SA 258 already in ingress list
    ```

6. Add the old ingress-sa.

    ```
    switch(config-if-esp)# ingress-sa 258
    ```

- CSCsq20408

    Symptom: The **show startup** command displays aspects of the running configuration when SANTap is configured and/or SANTap objects are created. When a user creates objects such as a CVT or DVT, the configuration is showing in the running-configuration and in the startup-configuration without copying the configuration into the startup-configuration.

Workaround: Issue a **copy running-config startup-config** command whenever you create objects such as a CVT or DVT so that the running-configuration and startup-configuration are synchronized.

- CSCsy37951

  Symptom: The Trunking F PortChannels feature is not available in NX-OS Release 4.1(1x); however, a downgrade from Release 4.1(3a) or later to Release 4.1(1x) is nondisruptive, even when the Trunking F PortChannels feature is enabled (using the **feature fport-channel-trunk** command) while running Release 4.1(3a) or later.

  Workaround: If a downgrade to Release 4.1(1x) is performed when the Trunking F PortChannels feature is enabled, the switch will be in an inconsistent state. You must reload the switch after a downgrade to Release 4.1(1x).

- CSCte93219

  Symptom: If you have an MDS 9000 switch running NX-OS Release 5.0(1a) and also running DMM or Secure Erase, when you downgrade to an NX-OS 4.x release, you see the following errors:

  - syslog messages display with the error string PSS_VERSION_MISMATCH for the configuration of an internal service (ilc_helper)

  - After the ISSD completes and the switch comes up with the NX-OS 4.x release, an internal process (ilc_helper) fails.

  Workaround: None

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/partner/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/partner/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 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 Release 4.1(x) and SAN-OS 3(x) 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.

Send documentation comments to mdsfeedback-doc@cisco.com