Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 4.1(3a)

Release Date: March 11, 2009

Part Number: OL-17675-05 Y0

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 55.

Note 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	03/11/2009	Created release notes.
B0	03/13/2009	Removed the Limitation "Upgrading an MDS 9222i Switch with an Active FC-Redirect Configuration."
C0	03/16/2009	Added DDTS CSCsy37951. Added Oracle 11g Enterprise Edition and Oracle 10g Enterprise Edition to the list of software supported by Cisco Fabric Manager and Device Manager, in the "Upgrading Your Version of Cisco Fabric Manager"section.
D0	03/18/2009	Added DDTS CSCsu23984.
E0	03/19/2009	Added DDTS CSCsy52780.
F0	03/26/2009	Added DDTS CSCsw95386. Corrected Table 12, "FICON Supported Releases" and "FICON Downgrade Paths".
G0	03/27/2009	Added DDTS CSCsy58106.

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

Table 1 Online History Change (continued)

Revision	Date	Description
H0	04/16/2009	Added "FICON Supported Releases and Upgrade Paths". Revised "FICON Downgrade Paths".
I0	04/24/2009	Added DDTS CSCsz01738. Added the "Compatibility of Fabric Manager and Data Mobility Manager" limitation.
J0	05/07/2009	Added DDTS CSCsz21804. Added a statement not to use Java 1.6 Update 13 to the "The Fabric Manager Installation Process Overview" section.
K0	06/04/2009	Added SAN-OS Release 3.3(3) to the Nondisruptive Software Upgrade Path information in Table 11 and to the Nondisruptive Software Downgrade Path information inTable 13. Added DDTS CSCsx32050.
L0	08/03/2009	Added DDTS CSCsu33302 and CSCtb00005. Updated Table 10 with upgrade path from 3.3.x to 4.1.x.
M0	08/31/2009	Added a Note to the "Installing Fabric Manager on Windows" section on page -18 about the effect of a Group Policy Object (GPO) in Windows on Fabric Manager Server when used with the PostgreSQL database.
N0	09/21/2009	Added DDTS CSCsy23429.
O0	11/11/2009	Added DDTS CSCtc48338.
P0	11/18/2009	Added DDTS CSCtb28442, CSCtb77695, and CSCtc20849.
Q0	12/10/2009	Added DDTS CSCsz59152.
R0	12/23/2009	Added DDTS CSCtc04286 and CSCtd16646.
S0	01/26/2010	AddedDDTS CSCsy73212 and CSCsz84411.
T0	04/14/2010	Added the"Determining Software Version Compatibility" section.
U0	07/29/2010	Added the "PPRC Not Supported with FCIP Write Acceleration" limitation.
V0	10/12/2010	Added DDTS CSCsv20465 and CSCtc65441. Added the Cisco MDS 9500 Series Supervisor-2A module to Table 2.
W0	11/09/2010	Added DDTS CSCta28484.
X0	12/17/2010	Removed CSCsv20465 which was resolved in MDS NX-OS Release 4.1(3).
Y0	03/12/2012	Updated Table 11 and Table 13.

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	M95S2K9-4.1.3a	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-4.1.3a	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M92S1K9-4.1.3a	MDS 9216i Supervisor/Fabric-I, NX-OS software	MDS 9216i Switch only
	M91S2K9-4.1.3a	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9124 Switch and MDS 9134 Switch
SSI Interface	SSI-M9K9-411A	Storage Services Interface for NX-OS Release 4.1(3a)	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
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

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-C9216i-K9	Cisco MDS 9216i Multilayer Fabric Switch (3RU semi-modular multilayer fabric switch with 14 2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9216i 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-X9016	Cisco MDS 9000 16-Port Fibre Channel Switching Module with Small Form-Factor Pluggable (SFP) LC (16-port, 2-Gbps Fibre Channel switching module with SFP LC connectors for Cisco MDS 9216i and Cisco MDS 9500 Series)	MDS 9500 Series MDS 9216i Switch
	DS-X9032	Cisco MDS 9000 32-Port 2-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9216i Switch
	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
Services Modules	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
	DS-X9302-14K9	Cisco MDS 9000 14/2-Port Multiprotocol Services Module — 14-port, 2-Gbps Fibre Channel plus 2-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDs 9216i Switch
	DS-X9032-SSM	Cisco MDS 9000 32-Port Storage Services Module — 32-port, 2-Gbps storage services 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

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

Component	Part Number	Description	Applicable Product
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 in Cisco MDS NX-OS 4.x

Table 3 lists the MDS hardware chassis supported by Cisco MDS NX-OS 4.x.

Table 3 Cisco MDS NX-OS 4.x Chassis Support Matrix

Switch	NX-OS 4.x Support
MDS 9513	Yes
MDS 9509	Yes
MDS 9506	Yes
MDS 9222i	Yes
MDS 9216i	Yes
MDS 9216A	No
MDS 9216	No
MDS 9134	Yes
MD S 9124	Yes
MDS 9140	No
MDS 9120	No
Cisco Fabric Switch for HP c-Class BladeSystem and Cisco Fabric Switch for IBM BladeCenter	Yes

Table 4 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 5.

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

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	No	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	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 4 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 5 lists the MDS hardware modules supported by Cisco MDS SAN-OS 3.x.

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

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	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-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes	Yes	No
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes	Yes	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes	Yes	Yes

Table 5 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-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

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 Family 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

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.

Note We strongly recommend that you use the latest available software release supported by your vendor for all Cisco MDS 9000 Family products.

Determining Software Version Compatibility

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

Table 6 Software Version Compatibility

NX-OS Release 5.0(x)	Compatible NX-OS 4.x Versions	Compatible SAN-OS 3.x Versions
NX-OS Release 5.0(1a)	Release 4.1(1b), 4.1(1c), 4.1(3), 4.1(3a), 4.2(1a), 4.2(1b), 4.2(3), 4.2(3a), 4.2(5). Release 4.1(1b) is the minimum supported version.	Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4), 3.3(4a), 3.3(5). Release 3.3(1c) is the minimum supported version.

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:1.3(x)_filename** command determines which additional features need to be disabled.

Note Refer to the "Determining Software Compatibility" section of the *Cisco MDS 9000 Family CLI Configuration Guide* for more details.

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 7.

Table 7 Software Images for MDS 9100 Series Switches

Cisco MDS 9100 Series Switch Type	Supervisor Module Type	Naming Convention
9124, 9134, Cisco Fabric Switch for HP c-Class BladeSystem, Cisco Fabric Switch for IBM BladeCenter	Supervisor-2 module	Filename begins with m9100-s2ek9

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 8.

Table 8 Software Images for MDS 9200 Series Switches

Cisco MDS 9200 Series Switch Type	Supervisor Module Type	Naming Convention
9222i	Supervisor-2 module	Filename begins with m9200-s2ek9
9216i		Filename begins with m9200-ek9

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series switch depends on whether the switch is based on a Supervisor-1 module or a Supervisor-2 module, as shown in Table 9.

Table 9 Software Images for Supervisor Type

Cisco MDS 9500 Series Switch Type	Supervisor Module Type	Naming Convention
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:

Note Before you begin the upgrade process, review the list of chassis and modules that Cisco MDS NX-OS Release 4.1(3a) supports. See the "MDS 9000 Chassis and Module Support in Cisco MDS NX-OS 4.x" section on page 10.

Installation Changes for Cisco Fabric Manager in This Release

Starting with Cisco MDS NX-OS Release 4.1(3a), Fabric Manager is installed in the $INSTALLDIR/dcm/fm directory.

$INSTALLDIR is the Fabric Manager installation directory. The default path to the directory is as follows:

- /usr/local/cisco on Linux/Solaris systems
- C:\Program Files\Cisco Systems on Windows systems

The database is installed in $INSTALLDIR/db and JBoss is in $INSTALLDIR/jboss-4.2.2.GA.

In addition, starting from NX-OS Release 4.1(3a), when you uninstall Fabric Manager Server, only Fabric Manager is removed. Jboss and the database, either PostgreSQL or Oracle, are not removed because they might be shared with other applications such as Cisco DCNM.

Upgrading Your Version of Cisco Fabric Manager

As of Cisco SAN-OS Release 3.2(1), Cisco Fabric Manager is no longer packaged with a Cisco MDS 9000 Family switch. It is included on the CD-ROM that ships with the switch. You can install Fabric Manager from the CD-ROM or from files that you download.

Installing Cisco Fabric Manager is a multi-step process that involves installing a database, as well as Fabric Manager. The complete installation instructions are provided in the "Installation of Cisco MDS NX-OS and Fabric Manager" section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide,* and are available on-screen once you launch the Fabric Manager installer from the CD-ROM.

Note When upgrading Fabric Manager, refer to the supported upgrade path shown in Table 10. For example, when upgrading from SAN-OS Release 3.1(x) to NX-OS Release 4.1(x), you will need to upgrade from Release 3.1(x) to Release 3.2(x) to Release 3.3(x) and then upgrade to NX-OS Release 4.1(x)

Table 10 Supported Fabric Manager Upgrade Paths

Current	Upgrade Path
3.0.x	3.1.x
3.1.x (HSQL)	3.2.x (Oracle)
3.1.x (HSQL)	3.2.x PostgreSQL
3.1.x (Oracle)	3.2.x (Oracle)
3.2.x (Oracle)	3.3.x (Oracle
3.2.x (PostgreSQL)	3.3.x (PostgreSQL)
3.3.x (Oracle)	4.1.x (Oracle)
3.3.x (PostgreSQL)	4.1.x (PostgreSQL)

Note Fabric Manager Server can not be installed on an Active Directory Server when using PostgreSQL, Fabric Manager servers are domain controllers and can not create local PostgreSQL user accounts.

The Fabric Manager Installation Process Overview

The following section presents the flow of the installation process at a high level. Review these guidelines before you begin the installation process.

Caution Windows 2000 is incompatible with Cisco Fabric Manager Release 4.1(3a). If you are currently running Windows 2000, we strongly recommend that you update your environment before you begin the installation of Fabric Manager. This section lists the supported software that has been tested with Cisco Fabric Manager. See Table 10 for the supported upgrade paths for Cisco Fabric Manager.

Step 1 Verify supported software. Cisco Fabric Manager and Device Manager have been tested with the following software:

- Windows 2003 SP2, XP SP2, Windows Vista
- Red Hat Enterprise Linux AS Release 4 (Nahant Update 6)
- Solaris (SPARC) 8, 9, and 10
- VMWare ESX 3.5:
- Virtual Operating System: Windows 2003 SP2
- Java Sun JRE and JDK 1.5(x) and JRE 1.6(x) are supported

Note Do not use Java 1.6 Update 13.

- Java Web Start 1.2, 1.0.1, 1.5, 1.6
- Firefox 1.5 and 2.0
- Internet Explorer 6.x, and 7.0
- Oracle 11g Enterprise Edition
- Oracle 10g Enterprise Edition
- Oracle Database 10g Express
- PostgreSQL 8.2 (Windows and Linux)
- PostgreSQL 8.1 (Solaris)
- Cisco ACS 3.1 and 4.0
- PIX Firewall
- IP Tables
- SSH v2
- Global Enforce SNMP Privacy Encryption
- HTTPS

Note Cisco Fabric Manager has not been officially tested on any 64-bit platforms. Currently, we support only 32-bit platforms.

Step 2 Ensure data migration when upgrading Cisco Fabric Manager from Cisco SAN-OS Releases 3.1(2b) and later.

If you are upgrading Cisco Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and later, be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle Database 10g Express to Oracle Database 10g Express. If you migrate the database from Oracle to Oracle, the schema is updated. Refer to Table 10 for information on the supported upgrade path.

Step 3 Ensure data migration when upgrading Cisco Fabric Manager from releases prior to Cisco NX-OS Releases 4.1(3a).

If you are upgrading Fabric Manager in a Cisco SAN-OS Release prior to 3.1(2b), be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or the Oracle Database 10g Express during the installation. The Fabric Manager Installer installs the PostgreSQL database on Windows. If you want to install the PostgreSQL database on Solaris or Linux, or if you want to install

the Oracle Database 10g Express database, follow the instructions in the "Installation of Cisco MDS SAN-OS and Fabric Manager" section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide.* Refer to Table 10 for information on the supported upgrade path.

Step 4 If you are upgrading a previous installation of Fabric Manager, make sure the previous installation is installed and running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved.

Step 5 Select the database.

If you want to use the Oracle Database 10g Express, you must install the database and create a user name and password before continuing with the Fabric Manager installation. We recommend the Oracle Database 10g Express option for all users who are running Performance Manager on large fabrics (1000 or more end devices).

If you want to install the PostgreSQL database, you must disable any security software you are running as PostgreSQL may not install certain folders or users. You must also log in as a Superuser before you start the installation.

Step 6 Install Fabric Manager from the CD-ROM or from files that you download from cisco.com at the following website: http://cisco.com/cgi-bin/tablebuild.pl/mds-fm.

Installing Fabric Manager on Solaris

This section describes how to install Fabric Manager on Solaris.

To install Fabric Manager on Solaris, follow these steps:

Step 1 Set Java 1.5 or 1.6 to the path that is to be used for installing Fabric Manager.

Step 2 Install the database that is to be used with Fabric Manager.

Step 3 Copy the Fabric Manager jar file **m9000-fm-4.1.3a.jar** from the CD-ROM to a folder on the Solaris workstation.

Step 4 Launch the installer using the following command:

```
java -Xms512m -Xmx512m -jar m9000-fm-4.1.3a.jar
```

Step 5 Follow the onscreen instructions provided in the Fabric Manager management software setup wizard.

Installing Fabric Manager on Windows

This section describes how to install Fabric Manager on Windows.

Note Fabric Manager Server can not be installed on an Active Directory Server when using PostgreSQL, Fabric Manager servers are domain controllers and can not create local PostgreSQL user accounts.

Note If you are running Fabric Manager Server on Windows and using the PostgreSQL database, you should examine your Windows Active Directory environment for organizational units (OUs) and make the change recommended below to ensure that Fabric Manager Server does not periodically stop working.

On a Windows system, the Microsoft Active Directory applies a Group Policy Object (GPO) to the

Fabric Manager Server. The GPO does not recognize the local user PostgreSQL because it is not in the GPO allow list. As a result, the GPO removes it, and the PostgreSQL database stops working.

To avoid this situation, you should move the Fabric Manager Server to its own OU and apply the same feature settings as the original OU, but remove the local user account to log in as a service.

If your server is running Terminal Services in Application mode, or if you are running Citrix Metaframe or any variation thereof, you need to issue the following command on the DOS prompt before installing Fabric Manager Server.

Step 1 Open a command-line prompt: **Start** > **Run**, then type **cmd** and press **Return**.

Step 2 At the command prompt type: **user /install**.

Note Do not close the command line window. This must remain open for the entire duration of the install.

The following is an example of the output of this command:

```
C:\Documents and Settings\user.domain>USER /INSTALL

User session is ready to install applications.
```

Step 3 Follow all steps needed to install Fabric Manager, Fabric Manager Server, and Device Manager. See the instructions later in this section.

Step 4 When the installation is complete, at the command prompt, type **user /execute** and press **Return**. Then type **exit** and press **Return**.

The following is an example of the output of this command:

```
C:\Documents and Settings\user.domain>USER /execute

User session is ready to execute applications.
```

To install Fabric Manager on Windows, follow these steps:

Step 1 Click the **Install Management Software** link.

Step 2 Choose **Management Software > Cisco Fabric Manager**.

Step 3 Click the **Installing Fabric Manager** link.

Step 4 Select the drive for your CD-ROM.

Step 5 Click the **FM Installer** link.

Step 6 Follow the onscreen instructions provided in the Fabric Manager Installer 4.1(3a).

Note If you have any folders open or Windows Explorer task windows open during the installation, you might see the following error message:

C:\Program Files\Cisco Systems\dcm\fm\help\shared\images\Thumbs.db (Access is denied)

To resolve this issue, close all open folders and open Windows Explorer task windows and restart the FM Installer.

Caution Windows 2000 is incompatible with Fabric Manager Release 4.1(3a). If you install Fabric Manager in a Windows 2000 environment, you are at risk of having an unstable Fabric Manager. We recommend that you exit the installation and update your environment. See "The Fabric Manager Installation Process Overview" section on page 16 for the list of supported software that has been tested with Cisco Fabric Manager. See Table 10 for the supported upgrade paths for Fabric Manager.

To install Device Manager on your workstation, follow these steps:

Step 1 Enter the IP address of the switch in the Address field of your browser.

Step 2 Click the **Cisco Device Manager** link in the Device Manager installation window.

Step 3 Click **Next** to begin the installation.

Step 4 Follow the onscreen instructions to complete the installation of Device Manager.

Note If you use a Java JDK instead of a JRE on Solaris, you might encounter a problem trying to install the Device Manager from a web browser. This can happen because the installer heap limit of 256 MB is not sufficient. If you have this problem, save the jnlp link as file, increase the heap limit to 512 MB, and run **javaws element-manager.jnlp** at the shell prompt.

General Upgrading Guidelines

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

Use the following guidelines when upgrading to Cisco MDS NX-OS Release 4.1(x):

- Install and configure dual supervisor modules.
- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- Be aware that you need to enable Telnet following the upgrade. See "Enabling Telnet Required After an Upgrade" section on page 22.
- 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 27.
- Follow the guidelines for upgrading a single supervisor switch as described in "Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch" section on page 28.
- Make note of the information concerning SANTap when performing upgrades on a Cisco MDS 9222i switch, as described in "Upgrading an MDS 9222i Switch with SANTap or Invista is Provisioned on the SSM" section on page 22.
- Be aware of the impact of an upgrade on VSAN 4079 if you are upgrading from SAN-OS Release 3.x to NX-OS 4.1(3a). See the "Upgrading Effect on VSAN 4079" section on page 22 for details.
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:
  - **Fibre Channel Ports**: Traffic on Fibre Channel ports can be nondisruptively upgraded. 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 24 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 23.

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 4.1(3a), 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.

Upgrading an MDS 9222i Switch with SANTap or Invista is Provisioned on the SSM

On an MDS 9222i switch, if SANTap or Invista is provisioned on a Storage Services Module (SSM) in slot 2, then an In Service Software Upgrade (ISSU) to NX-OS Release 4.1(3a) is not supported. The upgrade to NX-OS Release 4.1(3a) is supported if you set boot variables, save the configuration, and reload the switch. If the switch is running SAN-OS Release 3.3(1a) or earlier, first upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(3a).

Enabling Telnet Required After an Upgrade

Following an upgrade from SAN-OS 3.x to NX-OS 4.x, you need to enable the Telnet server if you require a Telnet connection. As of MDS NX-OS Release 4.1(1b), the Telnet server is disabled by default on all switches in the Cisco MDS 9000 Family. In earlier releases, the Telnet server was enabled by default.

Upgrading Effect on VSAN 4079

If you are upgrading from a SAN-OS Release 3.x to NX-OS Release 4.1(3a), 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, as shown in the following example:

```
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 4.1(3a) will have no affect on VSAN 4079.

If you downgrade after NX-OS Release 4.1(3) creates VSAN 4079 and reserves it for EVFP use, the VSAN will no longer be reserved.

Table 11 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 4.1(3a)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
Release 4.1(3), 4.1(1c), and 4.1(1b)	1. Upgrade to NX-OS Release 4.1(3a).
SAN-OS:	
Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	1. Upgrade to NX-OS Release 4.1(3a).
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)	1. Upgrade to SAN-OS Release 3.3(1c). 2. Upgrade to NX-OS Release 4.1(3a).
Release 2.1(2), 2.1(1b), 2.1(1a), and 2.0(x)	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(3a).
Release 1.x	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(3a).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 4.1(3a) 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 4.1(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)

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, and then follow the upgrade guidelines listed in the "Upgrading Your Version of Cisco Fabric Manager" section on page 16. 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.

Reconfiguring SSM Ports Before Upgrading to NX-OS Release 4.1(3a)

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode, which is the default for releases prior to Release 3.0(1).

Note To avoid any traffic disruption, modify the configuration of the SSM ports as described below, before upgrading a SAN-OS software image prior to Release 3.3(1c) to NX-OS Release 4.1(3a).

For more information on upgrading SAN-OS software, see the "Upgrading Your Cisco MDS NX-OS Software Image" section on page 15.

If the configuration is not updated before the upgrade, the installation process for the new image will automatically convert all ports configured in auto mode to Fx mode. This change in mode might cause a disruption if the port is currently operating in E mode.

To upgrade the image on your SSM without any traffic disruption, follow these steps:

Step 1 Verify the operational mode for each port on the SSM using the **show interface** command:

```
switch# show interface fc 2/1 - 32
fc2/1 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:4b:00:0d:ec:09:3c:00
    Admin port mode is auto             <-------- shows port is configured in auto mode
    snmp traps are enabled
    Port mode is F, FCID is 0xef0300    <-------- shows current port operational mode is F
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 3
```

Step 2 Change the configuration for the first port of the quad when the admin port mode is auto. (A quad is a group of four ports, supported by a data path processor (DPP). The groups are 1 to 4, 5 to 8, 9 to 12, and so on.) Do not leave the port mode set to auto.

a. Set the port admin mode to E or Fx if the current operational port mode is E, TE, F or FL.

```
switch# config t
switch(config)# interface fc 2/1
switch(config-if)# switchport mode fx
```

b. Set the port admin mode to E if the current operational port mode is E:

```
switch# config t
switch(config)# interface fc 2/5
switch(config-if)# switchport mode e
```

Step 3 Change the configuration for ports 2, 3, and 4 of the quad:

a. Set the admin port mode to Fx if the admin port mode of these ports is E, TE, or auto.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# switchport mode fx
```

b. If the first port in the port group has admin mode E or if the port is operational in E port mode, change the admin state of ports 2, 3, and 4 to shutdown.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# shutdown
```

Step 4 Save the running configuration to the startup configuration before the upgrade procedure to ensure that the changes are preserved during and after the upgrade. To save the configuration, enter the following command:

```
switch# copy running-config startup-config
```

Upgrading the SSI Image on Your SSM

Use the following guidelines to nondisruptively upgrade the SSI image on your SSM:

- Install and configure dual supervisor modules.
- SSM intelligent services traffic on SSM ports is disrupted during upgrades. Fibre Channel switching traffic is not disrupted under the following conditions:
  - Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images.*
  - All SSM applications are disabled. Use the **show ssm provisioning** command to determine what applications are configured. Use the **no ssm enable feature** command to disable these applications.
  - No SSM ports are in auto mode. See the "Reconfiguring SSM Ports Before Upgrading to NX-OS Release 4.1(3a)" section on page 25.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco Data Center Interoperability Support Matrix* and the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x,* for information on upgrading your SSM.

Caution Upgrading from Cisco MDS SAN-OS Release 2.1(1b) or earlier to Release 2.1.2 or later can disrupt traffic on any SSM installed on your MDS switch.

Upgrading a Switch with Insufficient Space for Two Images on the Bootflash

To upgrade the SAN-OS image on a Cisco MDS 9000 Family switch requires enough space on the internal CompactFlash (also referred to as bootflash) to accommodate both the old software image and the new software image.

As of Cisco MDS SAN-OS Release 3.1(1), on MDS switches with a 256-MB CompactFlash, it is possible in some scenarios that a user might be unable to fit two images on the bootflash. This lack of space on the bootflash might cause the upgrade process to fail because new images are always copied onto the bootflash during an upgrade.

The following MDS switches are affected by this issue:

- MDS 9216 and MDS 9216i
- MDS 9120 and MDS 9140
- MDS 9500 Series switches with a Supervisor 1 module

To work around an image upgrade failure caused by a lack of space on the bootflash, follow these steps:

Step 1 Prior to installing the new image, copy the old (existing) system image file to an external server. You may need to reinstall this file later.

Step 2 Delete the old system image file from the bootflash by using either the Fabric Manager install utility or the CLI **delete bootflash:** command. The system image file does not contain the word "kickstart" in the filename.

```
switch# delete bootflash:m9200-ek9-mz.3.0.3.bin
```

Note On MDS 9500 Series switches, you also need to delete the image file from the standby supervisor after deleting it from the active supervisor.

```
switch# delete  bootflash://sup-standby/m9500-sf1ek9-mz.3.0.3.bin
```

Step 3 Start the image upgrade or installation process using the Fabric Manager install utility or the CLI **install all** command.

Step 4 If the new installation or upgrade fails while copying the image and you want to keep the old (existing) image, then copy the old image (that you saved to an external server in Step 1) to the bootflash using either Fabric Manager or the **copy** command.

Step 5 If the switch fails to boot, then follow the recovery procedure described in the "Troubleshooting Installs, Upgrades, and Reboots" section of the *Cisco MDS 9000 Family Troubleshooting Guide, Release 3.x.*

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 4.1(x) 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 a Single Supervisor MDS Family Switch

Cisco MDS SAN-OS software upgrades are disruptive on the following single supervisor Cisco MDS Family switches:

- MDS 9120 switch
- MDS 9140 switch
- MDS 9216i switch

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path shown in Table 11, even though the upgrade is disruptive. Following the nondisruptive upgrade path ensures that the binary startup configuration remains intact.

If you do not follow the upgrade path, (for example, you upgrade directly from SAN-OS Release 2.1(2) or earlier version to NX-OS Release 4.1(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 an MDS 9120 switch or an MDS 9140 switch to Cisco NX-OS 4.x. See Table 3 for the list of switches that support Cisco NX-OS 4.x

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

Use the following guidelines to nondisruptively downgrade your Cisco MDS NX-OS Release 4.1(3a):

- 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**: Traffic on Fibre Channel ports can be nondisruptively downgraded. See Table 13 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 24 for these instructions.
  - **FICON**: If you have FICON enabled, the downgrade path is different. See the "FICON Downgrade Paths" section on page 30.

Note A downgrade from NX-OS Release 4.1(3a) 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 13 to determine the nondisruptive downgrade path from Cisco NX-OS Release 4.1(3a). 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 13 applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

Table 13 Nondisruptive Downgrade Path from NX-OS Release 4.1(3a)

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
Release 4.1(3), 4.1(1c), and 4.1(1b)	1. Downgrade to NX-OS Release 4.1(x).
SAN-OS:	
All 3.3(x) releases	2. Downgrade to NX-OS 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.	1. Downgrade to NX-OS Release 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. 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.	1. Downgrade to NX-OS Release 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. Downgrade to SAN-OS Release 2.1(2x). 4. Downgrade to SAN-OS Release 2.0(x).
Release 1.x	1. Downgrade to NX-OS Release 4 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. Downgrade to SAN-OS Release 2.1(2b). 4. Downgrade to SAN-OS Release 1.3(4a). 5. Downgrade to SAN-OS Release 1.x.

FICON Downgrade Paths

Cisco MDS NX-OS Release 4.1(3a) does not support FICON.

Refer to Table 12 for a list of SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON downgrade path information.

Downgrading the SSI Image on Your SSM

Use the following guidelines when downgrading your SSI image on your SSM:

- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco NX-OS Release 4.1(x) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
- SSM intelligent services traffic switching on SSM ports is disrupted on upgrades or downgrades.
- Fibre Channel switching traffic on SSM ports is not disrupted under the following conditions:
  - All SSM applications are disabled. Use the **show ssm provisioning** command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco Data Center Interoperability Support Matrix* and the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x,* for information on downgrading your SSM.

New Features in Cisco MDS NX-OS Release 4.1(3a)

This section briefly describes the new features introduced in this release. For detailed information about the features listed, refer to the *Cisco MDS 9000 Family CLI Configuration Guide,* the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, and the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*. For information about new commands associated with these features, refer to the *Cisco MDS 9000 Family Command Reference*. The "New and Changed Information" section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

Note These release notes are specific to this release. For the complete NX-OS and SAN-OS documentation set, see the "Related Documentation" section.

Cisco MDS 9000 NX-OS Release 4.1(3a) New Features

Cisco MDS 9000 NX-OS Release 4.1(3a) is a software release that includes new features, enhancements, and bug fixes. The most significant new features include the following:

Smart Call Home Enhancement

MDS 9000 Family switches previously required an e-mail gateway to send notifications. Starting from Cisco MDS NX-OS Release 4.1(3a), MDS switches are capable of sending notifications via https.

F port Trunking and F port Channeling with NPV

Cisco MDS NX-OS Release 4.1(3a) introduces F port trunking and F port channeling. These features are already available for E ports and are now available for F ports connected to NP ports on a switch where N port virtualization (NPV) is enabled. F port trunking allows multiple VSANs on a single uplink in NPV mode. Each physical blade server behind the NPV port can belong to a separate VSAN. Without F port trunking, the number of VSANs is limited to the number of physical uplink ports.

Using F port channeling with NPV, customers can take a group of F ports connected to NP ports on the NPV switch and group them as a single logical port. The feature provides both higher aggregate bandwidth for the NP link and greater resiliency. It also reduces the need for link reconfiguration triggered by broken links, failed ports, or module maintenance. Channeling is supported between NPV and core switches.

Port Owner

The port owner feature is intended for environments where there is more than one administrator. Port owner allows an administrator to mark some ports so that they appear as reserved in Device Manager. This feature can be used by one administrator to signal to another administrator that certain ports have been reserved.

Port Guard

Starting from NX-OS 4.1(3a), you can hold a port down after a failure or a series of flaps that are rapid enough to exceed a configured threshold. This capability can help keep the malfunctioning port down to avoid a flood of error reports.

Cisco Data Mobility Manager Enhancements

Cisco MDS NX-OS Release 4.1(3a) includes several enhancements to Cisco Data Mobility Manager (DMM).

Cisco Data Mobility Manager Method 3

Cisco Data Mobility Manger (DMM) is a feature that enables online migration of data from an existing storage array LUN to a new storage array LUN. Currently, there are two different methods available for the administrator to use this feature: method 1 and method 2. Method 1 provides synchronous replication for local and metro distances; Method 2 provides asynchronous replication that optimizes performance across a WAN link. Both these existing methods work in a dual fabric SAN topology. However there are customer topologies where a third SAN (or VSAN) is used to migrate the data from the existing to the new storage LUNs. Prior implementations of Cisco DMM did not support such three SAN (or VSAN) topologies. Cisco Data Mobility Manager Method 3 is a new method introduced in Cisco NX-OS Release 4.1(3a), that enables DMM to be used in topologies where there is a Dual Fabric SAN for server-to-storage Fibre Channel traffic and a third SAN (or VSAN) for migration traffic.

DMM Method 3 is available only on the MDS 900018/4-Port Multiservice Module (MSM-18/4).

Support for DMM on the MDS 9222i Switch

Starting with Cisco NX-OS Release 4.1(3a), the MDS 9222i Multiservice Modular Switch supports Cisco DMM without requiring an SSM module in the MDS 9222i switch.

Cisco Storage Media Encryption Enhancements

Cisco MDS NX-OS Release 4.1(3a) includes several enhancements to Cisco Storage Media Encryption (SME).

Media Key Auto-replication

Key replication is required to allow the same tape media to be accessed by more than one Cisco SME cluster. In most cases, these SME clusters are located in different locations, such as a primary data center and a disaster recovery site. Prior to Cisco NX-OS Release 4.1(3a), the key replication process required a manual export and import procedure, which limited the usefulness of the feature. Starting with NX-OS Release 4.1(3a), SME users can set up automatic replication of media keys from a Cisco SME cluster to one or more other clusters. Cisco SME media key auto-replication is configured on a per tape volume group basis.

Note The auto-replication source and destination clusters must be managed by a single Cisco Key Management Center (KMC).

High Availability KMC

Enhancements in Cisco NX-OS Release 4.1(3a) enable the KMC to be used in high availability environments where unattended operation is a requirement. The KMC can be configured to use an Oracle Enterprise database with Data Guard for redundancy. Both the primary KMC and secondary KMC are configured to point to the redundant database. Oracle maintains the key store synchronization and database availability.

A pair of KMCs is also required for high availability key management. Each SME cluster is aware of both the primary and secondary KMC. In the event that a SME cluster cannot reach the primary KMC, it automatically switches to the secondary. While using the secondary KMC, the SME cluster periodically checks to see if it can re-establish communications with the primary. The cluster resumes using the primary KMC once it is accessible again.

Cisco Fabric Manager Release 4.1(3a) New Features

Cisco Fabric Manager Release 4.1(3a) includes new features and enhancements.

Web Client Real-time Performance Charts

The Cisco Fabric Manager Server (FMS) web client performance charts have been enhanced to display real-time interface statistics in addition to the historical data.

Zone Database Backup Enhancements

The Cisco Fabric Manager Zone edit tool allows users to backup the zone database information. File Transfer Protocol (FTP), secure FTP (SFTP), and Secure Copy Protocol (SCP) are now supported in addition to Trivial File Transfer Protocol (TFTP) to back up the zone database.

Find in table Command

A find in table command has been added in Cisco NX-OS Release 4.1(3a) to locate rows in the Cisco Fabric Manager information table that is currently displayed. Users can use a next control to step between successive entries matching the find criteria.

Tools Menu Reorganization

The Cisco Fabric Manager Tools menu has been reorganized to group related tools under the following new submenus: Health, Connectivity, NPV, Data Mobility Manager, IP San, Security, and Install.

Flow Wizard List Filtering

The Fabric Manager Server flow wizard now allows new flow creation to be limited to a specific zone, rather than to an entire VSAN.

Fabric Manager Installer Changes

The following changes have been made to the Cisco Fabric Manager installer in Cisco NX-OS Release 4.1(3a):

- The Fabric Manager components shared with Cisco DCNM were relocated to a common directory.
- The Oracle JDBC component is no longer distributed with Fabric Manager.

Note If you require the Oracle JDBC component, you can download it from the Oracle Technology Network. You can download the recommended version (10.2.0.1.0) of the ojdbc14.jar file, from the following link:
http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_10201.html

Alternatively, if you have access to the system where Oracle is installed in your environment, you can find the jar file in the Oracle installation directory under ORACLE_HOME\jdbc\lib\.

For additional information about changes to the Fabric Manager installer, see the "Installation Changes for Cisco Fabric Manager in This Release" section on page 15.

Fabric Manager Platform Support

Cisco NX-OS Release 4.1(3a) is the last release to support Fabric Manager Solaris 8 and Red Hat Enterprise AS4 Linux.

Licensed Cisco NX-OS Software Packages

Most Cisco MDS 9000 family software features are included in the base configuration of the switch: 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 also are included in this package. Refer to the Cisco MDS 9000 Mainframe package fact sheet for more information.

Fabric Manager Server Package

The standard Cisco Fabric Manager and Device Manager applications bundled at no charge with the Cisco MDS 9000 family provide basic configuration and troubleshooting capabilities. The Cisco MDS 9000 FMS package extends Cisco Fabric Manager by providing historical performance monitoring for network traffic hotspot analysis, centralized management services, and advanced application integration for greater management efficiency. Refer to the Cisco MDS 9000 FMS 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 4-Gbps Cisco MDS 9100 Series Multilayer Fabric Switches. As needed, customers can expand switch connectivity by licensing additional ports.

Storage Media Encryption Package

The Cisco MDS 9000 Storage Media Encryption package enables encryption of data at rest on heterogeneous tape devices and virtual tape libraries as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 Family switches and the Cisco Fabric Manager 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.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility 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 Fabric Manager 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.

Limitations and Restrictions

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

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. This addresses the following:

1. 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.
2. This makes the Cisco MDS behavior consistent with other Cisco products such as Nexus 7000 which exhibits the same behavior for those roles (when they apply to the VLAN policy).

Data Mobility Manager

For a storage-based Data Mobility Manager (DMM) job that is in the Scheduled state, if the server HBA port goes offline, then the scheduled DMM job will not start. Scheduled DMM jobs start only when all server HBA ports and storage ports are up. For scheduled DMM jobs, make sure all server HBA ports and storage ports (both existing and new storage) are up.

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).

Solaris Windows Manager

Solaris Windows Manager does not resize windows correctly which effects some Device Manager screens. To resolve this, download and install the 119538-1 patch from Sun Microsystems. The patch (119538-17 GNONE 2.6.0: Windows Manager Patch, Generic, 2008/08/08) can be obtained from sunsolve.sun.com.

Upgrading to Recover Loss of Performance Manager Data

Caution You must upgrade to Fabric Manager Release 3.1(x) and then upgrade to a later release of Fabric Manager to avoid losing Performance Manager data. If data has been lost, follow the steps below to recover the data.

Step 1 Disable Performance Manager interpolation using Fabric Manager Web Client. Uncheck **Interpolate missing statistics**, then click **Apply**.

Step 2 Stop the Fabric Manager Server.

Step 3 Save the data file in the **$INSTALL_DIR** directory.

Step 4 Move the old RRD file into the **$INSTALL_DIR/pm/db** directory.

Step 5 Run **$INSTALL_DIR/bin/pm.bat m**.

Step 6 Restart Fabric Manager Server.

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.

Cisco Storage Media Encryption

The following limitations are described for Cisco SME:

Cisco SME Configuration Limits

Table 14 lists the Cisco SME configuration limits for this release.

Table 14 Cisco SME Limits

Configuration	Limit
Number of switches in the fabric	10
Number of clusters per switch	1
Switches in a cluster	4
Fabrics in a cluster	2
Modules in a switch	11
Cisco MSM-18/4 modules in a cluster	32
Initiator-Target-LUNs (ITLs)	1024
LUNs behind a target	32
Host and target ports in a cluster	128
Number of hosts per target	128
Tape backup groups per cluster	2
Volume groups in a tape backup group	4
Cisco Key Management Center (# of keys)	32K
Targets per switch that can be FC-redirected	32

Deleting Cisco SME Interfaces

A Cisco SME interface can be deleted from the cluster only after the interface is administratively shut-down and all related tasks associated with the interface shut-down are complete.

Emulex Driver Version

In some instances, the Emulex driver version 8.1.10.9 may set the task attribute to HEAD_OF_QUEUE instead of SIMPLE_QUEUE. Certain tape drives do not accept this attribute and may reject these commands. The Emulex driver version 8.1.10.12 does not have this issue.

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 4.1(3a) does not support RSA version 1 keys. As a result, if you upgrade to NX-OS Release 4.1(3a) 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.

Proceed with the upgrade to NX-OS Release 4.1(3a).

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 CallHome Information

In MDS NX-OS Release 4.1(3a), CFS cannot distribute the following CallHome 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 CallHome commands:

```
switch# show running-config callhome
> version 4.1(3)
> callhome
>   email-contact abc@cisco.com <mailto:abc@cisco.com>
>   phone-contact +14087994089
>   streetaddress xyxxyx
>   distribute
>   destination-profile testProfile
>   destination-profile testProfile format XML
```

```
>    no destination-profile testProfile transport-method email
>    destination-profile testProfile transport-method http
>    destination-profile testProfile http https://xyz.abc.com
>    destination-profile testProfile alert-group all
>    transport email smtp-server 64.104.140.134 port 25 use-vrf management
>    transport email from abc@cisco.com <mailto:abc@cisco.com>
>    enable
>    commit
```

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

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

To work around this issue, 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-C9216i-K9, Cisco MDS 9216i Multilayer Fabric Switch
- 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 Family CLI 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 F PortChannel 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 22 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.

Compatibility of Fabric Manager and Data Mobility Manager

Cisco Fabric Manager in any MDS NX-OS 4.1(x) release does not support Data Mobility Manager (DMM) in any SAN-OS 3.3(x) release or in any 3.2(x) release. To use the Cisco Fabric Manager GUI for DMM, both Fabric Manager and DMM must be running NX-OS or SAN-OS software from the same release series.

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 15 to determine the status of a particular caveat. In the table, "O" indicates an open caveat and "R" indicates a resolved caveat.

Table 15 Open Caveats and Resolved Caveats Reference

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.1(1c)	4.1(3a)
Severity 1		
CSCtc65441	—	O
Severity 2		
CSCsi72048	O	R
CSCsk11207	O	R
CSCsq78868	O	R
CSCsu31909	O	R
CSCsu33302	O	R
CSCsu84919	O	R
CSCsu98190	O	R
CSCsv27564	O	R
CSCsw95386	O	R
CSCsx63346	O	R
CSCsz21804	—	O
CSCsz84411	O	O
CSCsz59152	O	O
CSCtb00005	O	R
CSCtb28442	O	O
CSCtb77695	O	O
CSCtc20849	O	O
CSCtc48338	O	O
CSCtd16646	O	O
Severity 3		
CSCsk35725	O	O
CSCso63465	O	R
CSCsq20408	O	O

Table 15 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.1(1c)	4.1(3a)
CSCsr69166	O	R
CSCsu23984	O	R
CSCsu30034	O	R
CSCsu37199	O	R
CSCsu38297	O	R
CSCsu41818	O	R
CSCsu42003	O	R
CSCsu53299	O	R
CSCsu56780	O	R
CSCsu63218	O	R
CSCsu72195	O	O
CSCsu73264	O	R
CSCsu84511	O	R
CSCsu87264	O	R
CSCsu88059	O	R
CSCsv15452	O	R
CSCsv24238	O	R
CSCsv40524	O	R
CSCsw48060	O	R
CSCsw78035	O	R
CSCsx32050	—	O
CSCsx39090	O	R
CSCsy35135	—	O
CSCsy37951	—	O
CSCsy52780	—	O
CSCsy58106	—	O
CSCsy73212	—	O
CSCsz01738	—	O
CSCtc04286	O	O
Severity 4		
CSCsy23429	O	O
Severity 6		
CSCta28484	—	O

Resolved Caveats

- CSCsi72048

  Symptom: FCIP links may fail on an MDS 9216i switch that has compression set to auto when the other end of the FCIP link is terminated by an IPS-8 module. You may see the following message in the logs:

  ```
  %IPS_SB_MGR-SLOT1-3-CRYPTO_FAILURE: Heartbeat failure in encryption engine (error
  0x1)
  %ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface GigabitEthernet1/1 is down (Port
  software failure)
  %PORT-5-IF_DOWN_SOFTWARE_FAILURE: %$VSAN 1%$ Interface fcip99 is down (Port software
  failure)
  ```

  Workaround: This issue is resolved.

- CSCsk11207

  Symptom: Using Fabric Manager Web Client, you download Fabric Manager Client and when prompted to create a desktop shortcut, you select Yes. The default shortcut named “Cisco Fabric Manager” is created on the desktop. Then, using Fabric Manager Web Client again, you download another Fabric Manager Client from a different server (usually this will be a different version of Fabric Manager Client). You will not be prompted to create another shortcut because a desktop shortcut titled “Cisco Fabric Manager” already exists from the first installation.

  Workaround: This issue is resolved.

- CSCsq78868

  Symptom: Flow statistics on a Generation 2 module may not be accurate if any of the flows that participate in flow statistics on the module have multiple FSPF paths.

  Workaround: This issue is resolved.

- CSCsu31909

  Symptom: A failure in the internal software on the MSM-18/4 module causes an FCIP link in the PortChannel to drop.

  Workaround: This issue is resolved.

- CSCsu33302

  Symptom: An upgrade from NX-OS Release 4.1(1x) to NX-OS Release 4.2(1) might fail if the NX-OS Release 4.2(1) image takes longer to fully boot up than the time allocated by NX-OS Release 4.1(1x). If this occurs, you might see the following message:

  ```
  2009 Jul 28 10:29:56 emc-Fc-vegas2 %KERN-2-SYSTEM_MSG: mts_tcp_client_init():
  ret=-115, TCP HA SYNC connection to Standby Supervisor failed. Sock state=2,
  sk->state=1 - kernel
  2009 Jul 28 10:29:56 emc-Fc-vegas2 %KERN-2-SYSTEM_MSG: TCP connection to Standby
  failed with rc -115 - kernel
  ```

  The upgrade will abort and the standby supervisor will reload with the NX-OS Release 4.1(1x) image.

  Workaround: This issue is resolved.

- CSCsu84919

  Symptom: When hosts are continuously logging into virtual targets (VTs), the iSAPI process might leak memory which might cause the SSM to fail.

  Workaround: This issue is resolved.

- CSCsu98190

  Symptom: During an upgrade from Cisco MDS SAN-OS Release 3.3(1c) to Cisco NX-OS 4.1(1b) and later, applications might experience a very small amount of packet drops in the fabric. Most of the applications should be able to recover from such a small packet loss. The problem is seen only with an upgrade from SAN-OS Release 3.3(1c) and is not seen with an upgrade from either SAN-OS Release 3.3(1a) or SAN-OS Release 3.3(1b).

  Workaround: This issue is resolved.

- CSCsv27564

  Symptom: In rare cases, following a downgrade from an NX-OS 4.x image to a SAN-OS 3.x image, the available space on the bootflash might be displayed as less than the actual space that is available.

  Workaround: This issue is resolved.

- CSCsw95386

  Symptom: Certain applications that use SME perform a **move medium** operation to change tapes in a library, without first performing a **load** or **unload** operation. This causes the check condition "SCSI check condition of medium may have changed." SME does not perform the media identification logic correctly for this check condition, which causes tape labeling to fail.

  Workaround: This issue is resolved.

- CSCsx63346

  Symptom: If encryption is in use when you open a fabric, you cannot launch Device Manager from Cisco Fabric Manager.

  Workaround: This issue is resolved.

- CSCtb00005

  Symptom: On an MDS 9000 switch running NX-OS Release 4.1(x) software, if three supervisor switchovers occur within a 20-minute period, an embedded event manager (EEM) policy triggers the power down of all modules in the chassis. Internal processing associated with the EEM policy might leave the state of a module out-of-sync with the supervisor module.

  Workaround: This issue is resolved.

- CSCtc48338

  Symptom: On any of the MDS 9500 Series Director switches that have removable Supervisor 2 modules, a supervisor may reset when any one of the following commands is executed on the switch, or the same information is collected through Cisco Fabric Manager or Device Manager:

  - **show hardware internal mgmt0 stats**
  - **show hardware internal eobc stats**
  - **show tech**
  - **show tech details**
  - **show tech-support**
  - **tac-pac**

  In NX-OS Release 4.1(x) and Release 4.2(x), there are two additional commands that may cause this issue:

  - **show tech-support sysmgr**
  - **show tech-support ha**

  In a dual supervisor switch, entering one of these commands will force a supervisor switchover. In single supervisor systems, the switch will reload.

This issue does not affect switches with a nonremovable Supervisor 2 module, such as the MDS 9222i or MDS 9124.

Workaround: There are three ways that you can work around this issue:

- Do not enter the **show hardware internal mgmt0 stats** command or the **show hardware internal eobc stats** command.
- Upgrade to one of the following software releases when it becomes available:

  Cisco SAN-OS Release 3.3(4a) or above

  Cisco NX-OS Release 4.2(3) or above
- Before running the **show tech-support** command, the **show tech-support details** command, or the **tacpac** command from the CLI or from Cisco Fabric Manager or Device manager, download a plug-in from the Software Download Center to patch the commands. Load the plug-in on the active and standby supervisor as described in the following steps. The plug-in is not persistent across switchovers and should be loaded any time a switchover occurs.

To download and install the plug-in, follow these steps:

1. Download the plug-in from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282764109
2. Select release 1.0.
3. Make a copy of the downloaded gplug by entering the following command:
   switch# copy bootflash:m9500-sup2-showtech-FN63288-plugin-1.0.bin bootflash:gplug_copy
4. Copy the copy of the gplug to the standby supervisor by entering the following command:
   switch# **copy bootflash:gplug_copy bootflash://sup-remote/**
5. Load the gplug on the active supervisor by entering the following command:
   switch# **load bootflash:gplug_copy**
6. Attach to the standby supervisor by entering the following command:
   switch# **attach module** <standby-sup-slot>
7. Load the gplug onthe standby supervisor by entering the following command:
   switch# **load bootflash:gplug_copy**

For additional information, see the Field Notice FN - 63288 that is available at these links:

Guest: http://www.cisco.com/en/US/ts/fn/632/fn63288.html

Customer: http://www.cisco.com/en/US/customer/ts/fn/632/fn63288.html

- CSCtd16646

  Symptom: Bit errors occurred on frames received from the Cisco Fabric Switch for IBM BladeCenter on slots 1 through 4.

  Workaround: Upgrade to NX-OS Relase 4.2(3) where this issue is resolved.

- CSCso63465

  Symptom: FCP-CMD (for example, Inquiry) frames targeted to LUN 0x45F0 or LUN 0x50F0 are dropped by an MDS switch when traffic flows (egresses) through Generation 2 modules. LUN 0x45F0 corresponds to HPUX Volume Set Address <VBUS ID: 0xB, Target ID: 0xE, LUN: 0x0>.

  Workaround: This issue is resolved.

- CSCsr69166

  Symptom: Solaris Windows Manager does not resize windows correctly which effects some Device Manager screens.

Workaround: This issue is resolved.

- CSCsu23984

  Symptom: Starting with MDS NX-OS 4.1(1), a password security feature was introduced that allowed a user to enable a secure password standard. However, this feature was not being enforced for SNMP users.

  Workaround: This issue has been resolved.

- CSCsu30034

  Symptom: During and In Service Software Upgrade (ISSU), throughput statistics will not be available from the switch undergoing an upgrade. This information will be not able available from the CLI or Device Manager via SNMP.

  Workaround: This issue is resolved.

- CSCsu37199

  Symptom: Errors on the management port (mgmt0 or eth1) may be seen in the output of the sh**ow logging log** command.

  ```
  %KERN-3-SYSTEM_MSG: eth1: error in ethGetNextRxBuf %KERN-3-SYSTEM_MSG: eth1: stop
  internals failed %KERN-3-SYSTEM_MSG: eth1: error in rx %KERN-3-SYSTEM_MSG: eth1: error
  in rx %KERN-3-SYSTEM_MSG: eth1: error in rx %KERN-3-SYSTEM_MSG: eth1: error in rx
  %KERN-3-SYSTEM_MSG: eth1: error in rx
  ```

  In rare cases, this issue may result in a kernel panic which causes a supervisor switchover.

  Workaround: This issue is resolved.

- CSCsu38297

  Symptom: When performing a Veritas Netbackup database backup (such as a NB Catalog Backup), that requires a separate tape cartridge from the scratch pool (other than regular data backup tapes), the tape barcode is shown as Unknown in the Cisco Key Management Center.

  Workaround: This issue is resolved.

- CSCsu41818

  Symptom: Following a system reload with a startup-configuration that had scheduler configurations, none of the scheduler CLI commands are available. When upgrading to Cisco SAN-OS 3.2(1c) from a earlier version, the scheduler is enabled by default.

  Workaround: This issue is resolved.

- CSCsu42003

  Symptom: When an FCIP tunnel is configured with IPsec between an MDS 9222i switch and an MDS 9216i switch, it fails to come up if an ACL with TCP permit is configured. This causes a mismatch and causes the security association (SA) policy creation to fail in IPsec on the supervisor.

  Workaround: This issue is resolved.

- CSCsu53299

  Symptom: When reloading a switch, a timing condition may cause CFS to enter the handshake before the Routing Information Base (RIB) does. In this instance, CFS will not see any peers, and as a result, CFS-based applications will not communicate with the rest of the fabric.

  Workaround: This issue is resolved.

- CSCsu56780

  Symptom: A Solaris iSCSI host generates this error: iscsi: [ID 498442 kern.warning] WARNING: iscsi session(5) protocol error - received unknown itt:0x0 - protocol error.

Workaround: This issue is resolved

- CSCsu63218

  Symptom: In some cases, there may be duplicate entries of a global pWWN and virtual pWWN as identified in the following scenarios:

  - Switch 1 has a v1and p1 entry and p1 is connected to one of the server interfaces on switch 1.
  - Switch 2 also has a v1and p1 entry along with a v2 and p2 entry; and, switch 2 is in a different CFS region.
  - While using Replace on different switch option in the FA wizard, if v1 and p2 is provided in the step4 then, the expected operation won't be performed.

  Workaround: This issue is Resolved.

- CSCsu73264

  Symptom: Data Mobility Manager (DMM) uses VSAN 1 for IP communication and it requires **interface cpp**<*module*>**/1/1** to be configured. If another CPP IP Fibre Channel interface is configured in the same module in a different VSAN, then DMM will not work.

  Workaround: This issue is resolved.

- CSCsu84511

  Symptom: When a Cisco MDS switch is configured to use an AAA server using TACACS+ and with enabling the directed request option, a login using <user>@<server> provides the network-operator privilege instead of the actual privilege mentioned in the ACS server. This happens once AAA accounting is set to remote. A login without enabling the directed request option works as expected and provides the appropriate privilege. This issue does not exist when using the RADIUS protocol with the directed request option enabled.

  Workaround: This issue is resolved.

- CSCsu87264

  Symptom: The Cisco MDS 9000 Family 1/2/4/8-Gbps 24-Port FC Module (DS-X9224-96K9) and the Cisco MDS 9000 Family 1/2/4/8-Gbps 48-Port FC Module (DS-X9248-96K9) go to the OK state when plugged into a Cisco MDS 9216i switch. The MDS 9216i switch does not support these two modules in NX-OS Release 4.1(1b).

  Workaround: This issue is resolved.

- CSCsu90793

  Symptom: Software failures occurred on a Gigabit Ethernet port when FCIP compression mode auto was used.

  Workaround: This issue is resolved.

- CSCsu88059

  Symptom: After first installing Fabric Manager Server (FMS) (with default flag displayFCoE = false), and then stopping and restarting the FMS with displayFCoE = true, the FCoE interface tables are not showing when the old disconnected client re-connects. As a result, the following four FCoE menus do not launch the corresponding tables (FCOE, Virtual Interface Group, Virtual FC Interfaces, Virtual Ethernet Interfaces).

  Workaround: This issue is resolved.

- CSCsv15452

  Symptom: The Fabric Manager Server Performance Manager does not show fcflow statistics for all devices. The **Performance>Flows** window shows n/a values for the vast majority of devices in many VSANs.

  Workaround: This issue is resolved.

- CSCsv24238

  Symptom: If you have host to storage connectivity issues, check the following counters to see if you have increasing packet drops throughout the path that these devices traverse. Use the **show hardware internal packet-flow dropped** command and the **show hardware internal errors all** command to check the counters.

  Workaround: This issue is resolved.

- CSCsv40524

  Symptom: When a SNMP user makes any changes to the zone database, in enhanced zoning mode, the database is locked by the user. The zone dialog box when refreshed or launched will pop up a warning indicating the zone database is locked. If the locking SNMP user making the change is same as the SNMP user launching the zone dialog, this warning is not given (since this user can edit the zone database). The commit button is enabled for this user.

  Workaround: This issue is resolved.

- CSCsw48060

  Symptom: FCIP interoperability fails between two MDS switches, one running MDS NX-OS Release 4.1(1c) and the other running MDS NX-OS Release 4.1(3a), if the IP ACL configuration for an IPSec crypto map specifies TCP as the protocol, as in the following example:

  ```
  switch(config)# ip access-list acl-name permit tcp local-gige-ip-address local-mask
  remote-gige-ipaddress remote-mask
  ```

  FCIP interoperability does not fail if the IP ACL uses IP as the protocol, as in the following example:

  ```
  switch(config)# ip access-list acl-name permit ip local-gige-ip-address local-mask
  remote-gige-ipaddress remote-mask
  ```

  Workaround: This issue is resolved.

- CSCsw78035

  Symptom: When FlexAttach is enabled on the switch, the physical pWWN in the FCNS registration response is not rewritten with the virtual pWWN.

  Workaround: This issue is resolved.

- CSCsx39090

  Symptom: When you click **Resync Open Fabric** in Fabric Manager, the fabric configuration appears to be saved to the startup configuration, when in fact it is not saved. The same situation occurs when you exit Fabric Manager: the fabric configuration is not saved to the startup configuration.

  Workaround: This issue is resolved.

Open Caveats

- CSCtc65441

  Symptom: A watchdog timeout error may cause a Cisco MDS 9124 switch to fail and reload. This symptom may occur when there is excessive traffic or errors on the mgmt0 port.

  Workaround: Avoid overloading the mgmt0 port.

- CSCsz21804

  Symptom: After you perform an in-service software upgrade (ISSU) from SAN-OS Release 3.x to NX-OS Release 4.x, the **show fcs database** command does not display the attached pWWNs.

  Workaround: Enter a **shut** command, followed by a **no shut** command on the Fibre Channel interfaces on the switch. Then enter the **show fcs database** command to display the pWWNs.

- 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: Install and power up the redundant power supply.

- CSCsz59152

  Symptom: On an MDS 9513 switch, the crossbar ASIC on a Fabric 1 or Fabric 2 module may fail. As a result, some ports may get disabled on the modules that use the crossbar links in the bad fabric module.

  Workaround: To resolve this issue, follow these steps:

  1. Replace the affected Fabric 1 or Fabric 2 module.
  2. Manually bring up the ports that went down by entering the **shut** command, followed by the **no shut** command.

- CSCtb28442

  Symptom: End of sequence is not set for STK drives when the host requests more data than what is written to the tape.

  Workaround: None.

- CSCtb77695

  Symptom: When a tape reaches its capacity, an IBM TS1120 tape drive 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 the tape has not been reached. As a result, the backup fails when it spans across multiple tapes. This issue is specific only to IBM TS1120 tape drives.

  Workaround: None.

- CSCtc20849

  Symptom: Following a reboot of an MDS 9513 switch running Cisco SAN-OS Release 3.3(2), both supervisor modules generated core files. The **show cores** command and the **show system reset-reason** command displayed the following output:

```
switch# show cores
Module-num       Process-name      PID     Core-create-time
----------       ------------      ---     ----------------
8                qos               15671   Sep 21 22:16
7                qos               4370    Sep 21 22:17

switch# show system reset-reason
```

```
----- reset reason for Supervisor-module 8 (from Supervisor in slot 8) ---
1) At 517868 usecs after Mon Sep 21 22:12:09 2009
    Reason: Reset triggered due to HA policy of Reset
    Service: Service "qos"
    Version: 3.3(2)

----- reset reason for Supervisor-module 7 (from Supervisor in slot 7) ---
1) At 260648 usecs after Mon Sep 21 22:12:37 2009
    Reason: Reset triggered due to HA policy of Reset
    Service: Service "qos"
    Version: 3.3(2)
```

Workaround: To mitigate the risk of a QoS failure, configure static persistent FC IDs so that the local logins do not share the same domain or area. There should be no more than 50 logins with the same area.

In addition, you can enter the **show qos internal mem-stats detail | inc fcid** command and then check the current allocation value of the QOS_MEM_qos_fcid in the output. If this value is close to 70000, then there is a high chance of a QoS failure, followed by a system reboot.

- CSCsk35725

  Symptom: Fabric Manager takes 2 to 3 minutes to bring up the DMM job creation wizard in a setup with 25 switches, 400 enclosures, and 2400 entries in the name server.

  Workaround: None.

- 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.

- CSCsu72195

  Symptom: When replaying DMM job configurations saved as an ASCII text file (after performing a write erase), the DMM job includes discrepancies. These discrepancies occur due to the interface and zone configurations that are in an area below the DMM job configuration in the ASCII text file. The configurations stored in the ASCII text file are replayed sequentially from top to bottom.

  Workaround: None.

- CSCsx32050

  Symptom: If you use Fabric Manager to upgrade a switch from NX-OS Release 4.1(3a) to a higher release, Fabric Manager reports the status of a disruptive upgrade as **Failure:none**. If this situation occurs, you can log into the switch and verify if the upgrade actually did succeed. Enter the **show version** command to see if the switch reloaded and the new software version is running. If you perform the upgrade from the CLI, this situation does not occur.

  Workaround: None.

- CSCsy35135

  Symptom: Installing Fabric Manager and then installing Device Manager from Fabric Manager Server causes the Cisco Fabric Manager desktop shortcut and menu item to be changed to the Cisco Device Manager desktop shortcut and Cisco Device Manager menu item.

Workaround: To work around this issue, follow these steps:

1. On a Microsoft Windows machine, go to **Add or Remove Programs** and remove Cisco Device Manage and Cisco Fabric Manager if both programs are listed there.
2. Delete the Device Manager shortcut from your desktop.
3. Select **Start > All Programs > Cisco Fabric Manager,** right click and delete Cisco Fabric Manager.
4. Go to C:\Program Files\Cisco Systems and delete the dcm folder.
5. Go to C:\Documents and Settings\[user name], and delete the .cisco_mds9000 folder.
6. Select **Start >Control Panel >Java > General > Temporary Internet Files > View > Delete Device Manager and Fabric Manager > OK**.
7. Install Fabric Manager from the web client download window.
8. Open your fabric and go to **Map**. Click one of the switches to install Device Manager from the switch.

To avoid this problem, we recommend you do one of the following:

- Install Device Manager from a switch or a different Fabric Manager Server than you used to install the Fabric Manager Client.
- Install Device Manager before you install the Fabric Manager GUI Client.

- CSCsy37951

  Symptom: If you are running MDS NX-OS 4.1(3a) with the fport-channel-trunk feature enabled and you down grade to any NX-OS 4.1(1x) release, the installer performs a nondisruptive downgrade, even though the fport-channel-trunk feature is not supported in NX-OS 4.1(1x) releases. As a result, the switch is in an inconsistent state after the downgrade.

  Workaround: None.

- CSCsy52780

  Symptom: Occasionally, when you enter the **feature npv** command to enable NPV, or enter the **no feature npv** command to disable NPV, the switch does not reload as expected. Instead, it returns to the Configuration mode prompt.

  Workaround: If the switch returns to the Configuration mode prompt, enter the **reload** command. If you enter the **reload** command after entering the **feature npv** command, the switch will come up with NPV enabled. Likewise, if you enter the **reload** command after entering the **no feature npv** command, the switch will come up with NPV disabled.

- CSCsy58106

  Symptom: When dual supervisor modules are installed on a Cisco MDS switch running Cisco NX-OS Release 4.1(3a), if the feature fport_channel_trunk command has been issued to enable the F PortChannel feature and a switchover is performed, new F port trunking and F port channeling configurations cannot be made and the existing links may not come up if they flap after a switchover.

  Workaroud: With the F PortChannel feature enabled, reload the standby supervisor module and then perform the switchover.

- CSCsy73212

  Symptom: Under rare conditions, a port may drop data after the port flaps in the presence of congestion. The output of the **show hardware internal packet-flow dropped** command shows the dropped data as RX (receive) frame drops on a module. In such instances, the following type 1, type 2, and possibly type 3 errors may be seen:

  - Type 1 errors are internal ASIC parser CRC errors.
  - Type 2 errors are internal ASIC overflow or ECC parity errors.
  - Type 3 errors may occur when ports on a DS-X9124 or DS-X9148 module are put into a hardware failure state by the software. If all ports fail in this fashion, then the software reloads the module. If only some of the ports fail, the module is not reloaded.

  For this issue to occur, the port must have frames held in the port buffer at the time that the port is brought down and up. A port normally has time to empty its buffers when it is shut down. However, in unusual cases, such as if there is congestion on the port at the time of the shutdown, or in rare cases, frames can still be held in the buffers while the port is reinitialized.

  Workaround:None. If you experience this issue, check the fabric for congestion and then remove the congestion. Reload the module to recover ports that are in a hardware failure state.

- CSCsz01738

  Symptom: A host that is behind a NPIV F port cannot see the zoned LUNs if the addition of the F port to the zone and the zone set activation occur after an In Service Software Upgrade (ISSU). This issue applies only to an NPIV F port on MDS 9124 and MDS 9134 fabric switches

  Workaround: Following the ISSU, enter the **shut** command followed by the **no shut** command on the NPIV F port, and then activate the zone set.

- CSCtc04286

  Symptom: During bring up of the switch port, the port may go into an error disabled state with the reason “excessive interrupts.” This situation can occur if the other end that is connected to the port continuously sends OLS or NOS primitives.

  Workaround: To recover from the failure, enter the **shut** command, followed by the **no shut** command for the port. The switch will attempt to bring up the port again.

- CSCsy23429

  Symptom: Cross site scripting (XSS) issues exist in Fabric Manager Server when the Microsoft Internet Explorer web browser is used for web client management.

  Workaround: None.

- CSCta28484

  Symptom: On a Cisco MDS 9000 switch that is running Cisco NX-OS Release 4.x software, call home emails are not generated for link failures such as the following:

  ```
  %PORT-5-IF_DOWN_LINK_FAILURE: %$VSAN 36%$ Interface fc2/13 is down (Link failure)
  ```

  Workaround: For ports where you wish to receive a call home message for link failures,

  configure RMON to trigger an alert when a link failure occurs. RMON will in turn generate a call home message, provided that the RMON alert group is part of the call home destination profile.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at: http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.ht.

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website.

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco 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*

Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

Regulatory Compliance and Safety Information

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

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 Multilayer Fabric Switch Quick Start Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*

Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*

- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

Intelligent Storage Networking Services

- *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 - For Cisco MDS 9500 and 9200 Series*

Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*

Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

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.