Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 4.2(3)

Release Date: December 08, 2009

Part Number: OL-19964-04 O0

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 45.

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

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

Table 1 shows the on-line change history for this document.

Table 1 Online History Change

Revision	Date	Description
A0	12/08/2009	Created release notes.
B0	12/16/2009	Added DDTS CSCtc04286.
C0	12/18/2009	Added DDTS CSCtd16646.
D0	01/26/2010	Added DDTS CSCsz84411.
E0	04/12/2010	Added the "Determining Software Version Compatibility" section.
F0	07/27/2010	Added the "PPRC Not Supported with FCIP Write Acceleration" limitation.

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

Table 1 Online History Change (continued)

Revision	Date	Description
G0	10/12/2010	Added DDTS CSCtc65441. Added the Cisco MDS 9500 Series Supervisor-2A module to Table 2.
H0	11/09/2010	Added DDTS CSCta28484.
I0	02/09/2011	Updated the "Licensed Cisco NX-OS Software Packages" section.
J0	04/29/2011	• Updated the upgrade path to Release 4.2(3) from 4.1(1x) releases in Table 10. • Added DDTS CSCtn68418 as an Open Caveat.
K0	05/11/2011	Corrected the upgrade path to Release 4.2(3) in Table 10.
L0	09/09/2011	Added the "Configuring a Persistent FCID in an IVR Configuration with Brocade Switches" section.
M0	03/11/21012	Updated Table 10 and Table 13.
N0	05/03/2012	• Updated Table 10. • Added open caveat CSCty32238.
O0	05/18/2012	Added the "Converting Automatically Created PortChannels Before an Upgrade" section.

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	M95S2K9-4.2.3	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-4.2.3	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M92S1K9-4.2.3	MDS 9216i Supervisor/Fabric-I, NX-OS software	MDS 9216i Switch only
	M91S2K9-4.2.3	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9124 Switch and MDS 9134 Switch
SSI Interface	SSI-M9K9-423	Storage Services Interface for NX-OS Release 4.2(3)	MDS 9000 Family
Licenses	M9500SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9500 Series only
	M9222ISSE1K9	Storage Services Enabler License	MDS 9222i Switch only
	M9200SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9500 Series only
	M9222IDMMK9	Data Mobility Manager License for Cisco MDS 9222i	MDS 9222i Switch
	M92DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9200 Series only

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

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

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

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	Cisco MDS 9513 Multilayer Director (13-slot multilayer director with 2 slots for Supervisor-2 modules, with 11 slots available for switching modules — SFPs sold separately)	MDS 9513 Switch
	DS-C9509	Cisco MDS 9509 Multilayer Director (9-slot multilayer director with 2 slots for Supervisor modules, with 7 slots available for switching modules — SFPs sold separately)	MDS 9509 Switch
	DS-C9506	Cisco MDS 9506 Multilayer Director (6-slot multilayer director with 2 slots for Supervisor modules, with 4 slots available for switching modules — SFPs sold separately)	MDS 9506 Switch
	DS-C9222i-K9	Cisco MDS 9222i Multilayer Fabric Switch (3-rack-unit (3RU) semimodular multilayer fabric switch with 18 4-Gbps Fibre Channel ports, 4 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9222i Switch
	DS-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-X9316-SSNK9	Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16) — 16 fixed 1-Gbps Ethernet ports, plus 4 service engines that support 4 Gigabit Ethernet IP storage services ports.	MDS 9500 Series MDS 9222i Switch
	DS-X9304-18K9	Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) — 18-port, 4-Gbps Fibre Channel plus 4-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	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 9134	Yes
MD S 9124	Yes
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-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	No
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes

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

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
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-X9316-SSNK9	16-port Storage Services Node (SSN-16)	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes	Yes	No
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes	Yes	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	Yes	No	Yes	Yes	Yes
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	Yes	Yes	Yes	Yes	Yes

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

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

Caution Migrating your supervisor modules is a disruptive operation.

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

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

Software Download Process

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

Determining the Software Version

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 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 4.2(3) supports. See the "MDS 9000 Chassis and Module Support in Cisco MDS NX-OS 4.x" section on page 10.

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

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

General Upgrading Guidelines

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

Use the following guidelines when upgrading to Cisco MDS NX-OS Release 4.2(3):

- 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 19.
- 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 22.
- 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 23.
- 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 19.
- Be aware of the impact of an upgrade on VSAN 4079 if you are upgrading from SAN-OS Release 3.x to NX-OS 4.2(3). See the "Upgrading Effect on VSAN 4079" section on page 19 for details.
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:
  - **Fibre Channel Ports**: Traffic on Fibre Channel ports can be nondisruptively upgraded. See Table 10 for the nondisruptive upgrade path for all NX-OS and SAN-OS releases.
  - **SSM**: Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.
  - **Gigabit Ethernet Ports**: Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
  - **Inter-VSAN Routing (IVR)**: With IVR enabled, you must follow additional steps if you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the "Upgrading with IVR Enabled" section on page 19 for these instructions.
  - **FICON**: If you have FICON enabled, the upgrade path is different. See the "FICON Supported Releases and Upgrade Paths" section on page 17.

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 10 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 4.2(3), 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 10 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

Table 10 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 4.2(3)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
All 4.2(x) releases and all 4.1(x) releases	Upgrade to NX-OS Release 4.2(3).
SAN-OS:	
Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	Upgrade to NX-OS Release 4.2(3).
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 4.2(3).
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 4.2(3).
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 4.2(3).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 4.2(3) is not a FICON-qualified release.

Table 11 lists additional SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

Table 11 FICON Supported Releases

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

Use Table 12 to determine your FICON nondisruptive upgrade path to Cisco MDS NX-OS Release 4.2(1b) Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and follow the recommended path.

Table 12 FICON Nondisruptive Upgrade Path to MDS NX-OS Release 4.2(1b)

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

Upgrading 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 4.2(1b) is not supported. The upgrade to NX-OS Release 4.2(1b) 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 4.2(1b).

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 4.2(1b), 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 4.2(1b) will have no affect on VSAN 4079.

If you downgrade after NX-OS Release 4.2(1b) creates VSAN 4079 and reserves it for EVFP use, the VSAN will no longer be reserved.

Upgrading with IVR Enabled

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reconfiguring SSM Ports Before Upgrading to NX-OS Release 4.2(3)

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 4.2(1b).

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 4.2(3)" section on page 20.
  - 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 NX-OS Fundamentals Configuration Guide* for information on upgrading your SSM.

Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch

If you are upgrading from Cisco MDS SAN-OS Release 3.1(1) to Cisco NX-OS Release 4.2(1b) 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 Cisco MDS 9216i switch, which has a single supervisor. If you are performing an upgrade on this switch, you should follow the nondisruptive upgrade path shown in Table 10, 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 4.2(x)), the binary startup configuration is deleted because it is not compatible with the new image, and the ASCII startup configuration file is applied when the switch comes up with the new upgraded image. When the ASCII startup configuration file is applied, there may be errors. Because of this, we recommend that you follow the nondisruptive upgrade path.

Note You cannot upgrade 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.

Resetting SNMP Notifications Following an Upgrade

The SNMP notification configuration resets to the default settings when you upgrade to Cisco NX-OS Release 4.2(1b). Use the **snmp-server enable traps** command to reenable your required SNMP notifications.

Converting Automatically Created PortChannels Before an Upgrade

Before upgrading from NX-OS Release 4.1(x) or 4.2(x) to Release 5.x, ensure that you do not have any automatically created PortChannels present in the switch configuration. Use the **port-channel persistent** command to convert an automatically created PortChannel to a persistent PortChannel. Failure to convert automatically created PortChannels prior to the upgrade can result in traffic disruption because Autocreation of PortChannels is a deprecated feature as of NX-OS Release 4.1(1b).

Downgrading Your Cisco MDS SAN-OS Software Image

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

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS NX-OS Release 4.2(1b):

- 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 19 for these instructions.
  - **FICON**: If you have FICON enabled, the downgrade path is different. See the "FICON Downgrade Paths" section on page 25.

Note A downgrade from NX-OS Release 4.2(3) 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 4.2(1b). Find the SAN-OS image you want to downgrade to in the To SAN-OS Release column of the table and use the path recommended.

Note The software downgrade information in Table 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 4.2(3) a

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
All 4.2(x) and 4.1(x) releases	Downgrade to NX-OS Release 4.2(x) or 4.1(x).
SAN-OS:	
All 3.3(x) releases	1. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 2. 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 4.2(x) or 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 4.2(x) or 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 4.2(x) or Release 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

Table 14 lists the downgrade paths for FICON releases. Find the image release number that you want to downgrade to in the To Release with FICON Enabled column of the table and follow the recommended downgrade path.

Table 14 FICON Downgrade Path from NX-OS Release 4.2(1b)

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

Table 14 FICON Downgrade Path from NX-OS Release 4.2(1b) (continued)

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

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.

Downgrading an MDS 9500 Series Switch with an 8-Gbps Module Installed

If you attempt to perform a nondisruptive software downgrade from NX-OS Release 4.x to SAN-OS Release 3.x on an MDS 9500 Series switch that has an 8-Gbps module installed, the switch should display a message that the module is unsupported and stop the downgrade. Instead, the switch displays a message that the module is unsupported and proceeds with a disruptive downgrade. The following table shows the actual and expected behavior of the switch for a software downgrade.

Table 15 Downgrade Behavior on an MDS 9500 Series Switch with 8-Gbps Module Installed

Crossbar Fabric Mode	Switch Type	Software Version	Downgrade Software Version	Actual Install Behavior	Expected Install Behavior
DB mode[1]	MDS 9513 with 8-Gbps module	4.2(3)	3.3(x)	Disruptive	Abort. Disruptive after powerdown of 8-Gbps module.
DB mode	MDS 9513 without 8-Gbps module	4.2(3)	3.3(x)	Disruptive	Disruptive.
BM mode[2]	MDS 9513 with 8-Gbps module	4.2(3)	3.3(x)	Abort	Abort. Nondisruptive after powerdown of 8-Gbps module.
BM mode	MDS 9513 without 8-Gbps module	4.2(3)	3.3(x)	Nondisruptive	Nondisruptive.
BM mode	MDS 9509 or 9506 with 8-Gbps module	4.2(3)	3.3(x)	Abort	Abort. Nondisruptive after powerdown of 8-Gbps module.
BM mode	MDS 9509 or 9506 without 8-Gbps module	4.2(3	3.3(x)	Nondisruptive	Nondisruptive.

1. DB mode is the fabric mode that supports Generation 3 8-Gbps modules in an MDS 9513 switch chassis.
2. BM mode is the fabric mode that does not support Generation 3 8-Gbps modules in an MDS 9513 switch chassis.

New Features in Cisco MDS NX-OS Release 4.2(3)

There are no new features in Cisco MDS NX-OS Release 4.2(3).

Licensed Cisco NX-OS Software Packages

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

Enterprise Package

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

SAN Extension over IP Package

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

Mainframe Package

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

Storage Services Enabler Package

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

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco NX-OS Software features while initially purchasing only a small number of activated ports on 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. The Storage Media Encryption package is for use only with Cisco MDS 9000 Family switches.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility Manager package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or rewiring or reconfiguring SANs. Cisco DMM allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data verification, dual Fibre Channel fabric support, and management using Cisco 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. The Data Mobility Manager package is for use only with Cisco MDS 9000 Family switches.

I/O Accelerator Package

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

XRC Acceleration License

The Cisco Extended Remote Copy (XRC) acceleration license activates FICON XRC acceleration on the Cisco MDS 9222i switch and on the MSM-18/4 in the Cisco MDS 9500 Series directors. One license per chassis is required. You must install the Mainframe Package and the SAN Extension over FCIP Package before you install the XRC acceleration license. The Mainframe Package enables the underlying FICON support, and the FCIP license or licenses enable the underlying FCIP support. XRC acceleration is not supported on the SSN-16.

Limitations and Restrictions

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

IPv6

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

User Roles

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

prevented from performing **configuration**, **clear**, **execute**, and **debug** commands as before, however, they are allowed to perform **show** commands for all VSANs. The ability to execute the **show** command addresses the following:

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

Red Hat Enterprise Linux

The Linux kernel core dump is not supported in NX-OS Release 4.1(1b) and later versions and therefore the CLI command has been removed. A syntax error message will be displayed if you import configurations from SAN-OS Release 3.3(x) and earlier to NX-OS Release 4.1(1b) and later. These syntax errors do not affect the application of other commands in the configuration and can be safely ignored. To address this, remove the kernel core configuration from the ASCII configuration file before importing the configuration.

Generation 1 Module Limitation

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

Schedule Job Configurations

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

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

Maximum Number of Zones Supported in Interop Mode 4

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

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

InterVSAN Routing

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

Java Web Start

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

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

VRRP Availability

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

Using a RSA Version 1 Key for SSH Following an Upgrade

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

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

Step 1 Disable SSH.

Step 2 Create RSA version 2 DSA keys.

Step 3 Enable SSH.

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

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

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

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

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

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

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

CFS Cannot Distribute All Call Home Information

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

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

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

```
switch# show running-config callhome
> version 4.1(3)
> callhome
>   email-contact abc@cisco.com <mailto:abc@cisco.com>
>   phone-contact +14087994089
>   streetaddress xyxxyx
>   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 NX-OS Interfaces Configuration Guide*.

Reserved VSAN Range and Isolated VSAN Range Guidelines

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

- If trunk mode is on for any of the interfaces or NP PortChannel is up, the reserved VSANs are 3040 to 4078, and they are not available for user configuration.
- The Exchange Virtual Fabric Protocol (EVFP) isolated VSAN is 4079, and it is not available for user configuration.
- VSAN 4079 will be impacted by an upgrade to NX-OS Release 4.1(3a), depending on whether or not VSAN 4079 was created prior to the upgrade. See the "Upgrading Effect on VSAN 4079" section on page 19 for details.

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

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

Applying Zone Configurations to VSAN 1

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

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

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

Running Storage Applications on the MSM-18/4

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

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

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

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

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

I/O Accelerator Feature Limitations

In NX-OS Release 4.2(1b), IOA does not support the following NX-OS features:

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

Support for FCIP Compression Modes

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

Saving Copies of the Running Kickstart and System Images

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

Configuring Buffer Credits on a Generation 2 or Generation 3 Module

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

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

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

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

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

PPRC Not Supported with FCIP Write Acceleration

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

Configuring a Persistent FCID in an IVR Configuration with Brocade Switches

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

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

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

Caveats

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

Table 16 Open Caveats and Resolved Caveats Reference

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.2(1b)	4.2(3)
Severity 1		
CSCtc65441	O	O
Severity 2		
CSCsz84411	O	O
CSCtb74201	O	R
CSCtc11037	O	R
CSCtc20849	O	R
CSCtc21054	O	R
CSCtc41625	O	R
CSCtc48338	O	R
CSCtc55224	O	R
CSCtd16646	O	R
CSCtd59553	O	R
CSCty32238	O	O
Severity 3		
CSCsq20408	O	O
CSCsy37951	O	O
CSCtb49873	O	R
CSCtb62488	O	R
CSCtb89630	O	R
CSCtb99267	O	R
CSCtc03274	O	R
CSCtc04286	O	R
CSCtc33466	O	R
CSCtc41865	O	R
CSCtc47803	O	R
CSCtc54974	O	R
CSCtc58121	O	R
CSCtc68983	O	R
CSCtc77906	O	R

Table 16 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.2(1b)	4.2(3)
Severity 4		
CSCtc22830	O	R
CSCtn68418	—	O
Severity 6		
CSCsh64824	O	R
CSCsi33045	O	R
CSCta28484	O	R
CSCtb80346	O	R
CSCtc85276	O	R

Resolved Caveats

- CSCtb74201

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

  Workaround: This issue is resolved.

- CSCtc11037

  Symptom: In rare situations, if you enter the **show tech-support acl** command, a module may experience a CPU hog, which then causes the module to reload.

  Workaround: This issue is resolved.

- CSCtc20849

  Symptom: A module reboots because of a QoS failure. You may see this symptom when the number of local logins on a switch (typically on a director class) is very high (about 400) and if most of these logins share the same domain and area portion of the FC ID.

  Workaround: This issue is resolved.

- CSCtc21054

  Symptom: Sometimes a nondisruptive software upgrade on the Cisco Fabric Switch for IBM BladeCenter failed with the following reason: New IBM chassis type detected during the upgrade.

  Workaround: This issue is resolved.

- CSCtc41625

  Symptom: If IOA receives a data stream that cannot be compressed, and if the batch of data accumulated by IOA aligns to an internal buffer size, the IOA service engine will reset.

  Workaround: This issues 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), two additional commands are affected:

  - **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: This issue is resolved.

- CSCtc55224

  Symptom: If the UAP (Unique Area Port) assigns zero for the pWWN, the domain representing AFID and VSAN (DRAV) will reject a virtual FC ID with area allocation 0 and port ID 0, and return the error ZERO_AREA_PORT.

  Workaround: This issue is resolved.

- CSCtd16646

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

  Workaround: This issue is resolved.

- CSCtd59553

  Symptom: Disruption of regular traffic flows and IVR traffic flows on Fx ports, and disruption of IVR traffic flows on XE ports can occur when in-order-guarantee is enabled on a switch, and the following conditions are met:

  - Traffic is entering through a Generation 2 or Generation 3 module
  - Routes with multiple equal cost paths have PortChannel interfaces in use

  Workaround: This issue is resolved.

- CSCtb49873

  Symptom: Following several software upgrades, the VSAN information for a PortChannel member sometimes changes from the configured VSAN to the default VSAN. Because of this, any traps or syslogs that the port sends will be for a different VSAN rather than the port VSAN of the PortChannel to which it belongs.

  This issue occurs rarely and it has no operational impact other than the syslogs and accounting logs show a different VSAN for the particular port.

Workaround: This issue is resolved.

- CSCtb62488

  Symptom: A zoning state change gets stuck when there are over 2500 source and destination FC ID pair entries that need to be programmed for a given interface.

  Workaround: This issue is resolved.

- CSCtb89630

  Symptom: When setting up a DMM job, the existing storage LUNs cannot be seen for LUNs controlled by a Microsoft Cluster Server (MSCS) cluster. Existing storage LUNs can be seen with standalone servers.

  Workaround: This issue is resolved.

- CSCtb99267

  Symptom: When you create a DMM job, if the LUN size is more than one terabyte, the GUI displays the LUN size as 0.

  Workaround: This issue is resolved.

- CSCtc03274

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

  Workaround: This issue is resolved.

- 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: This issue is resolved

- CSCtc33466

  Symptom: When you copy an active zone set to full zone set, the copy operation will not succeed if the zone ID or zone name of the active zone set database and full zone set database are the same. This symptom was seen when an IVR zone merge was performed between two fabrics, where each fabric already had an active local IVR VSAN topology with an active IVR zone set. The IVR zone merge was successful, and the IVR zoning process worked as expected. A new active zone set was created with a concatenated IVR zone set and two IVR zone sets in the full zone set. However, when the **ivr copy active-zoneset full-zonese**t command was entered, the full IVR zone set was not overwritten.

  Workaround: This issue is resolved.

- CSCtc41865

  Symptom: During a software upgrade or a reload of the Cisco MDS 9000 MSM-18/4 module or the Cisco MDS 9000 SSN-16 module, IOA flows that are bound to the module are migrated to another IOA service engine in the fabric. The migration causes IOA to trigger a re-login of the host to the target. This process takes several seconds to complete. Certain devices do not tolerate the delay and do n**o**t re-login to the target. These devices require a manual intervention to re-login.

  This issue has been observed only in certain storage arrays involved in remote replication applications. Host drivers involved in tape backup environments do not exhibit this issue.

Workaround: This issue is resolved.

- CSCtc47803

  Symptom: Importing a volume group with greater than 500 keys fails with a browser error. As a result, the same set of keys are imported twice.

  Workaround: This issue is resolved.

- CSCtc54974

  Symptom: The password of the logged in SNMP user is visible in plain text in the Device Manager log. You might see this symptom whenever you start Device Manager and open the log window.

  Workaround: This issue is resolved.

- CSCtc58121

  Symptom: The MDS 9124 switch and the MDS 9222i switch show high memory usage, even though there is very little traffic or port utilization on the switch and the CPU is 100% idle.

  Workaround: This issue is resolved.

- CSCtc68983

  Symptom: After an upgrade from SAN-OS Release 3.0(2a) to Release 3.3(2), IVR zone set activation does not succeed. The following message was displayed:

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

  Following the upgrade to SAN-OS Release 3.3(2), the internal IVR device update database was found to have a missing entry for the device, which caused it to be stuck in the advertising state.

  Workaround: This issue is resolved.

- CSCtc77906

  Symptom: When a minor hardware issue with a backplane signal occurs, it can expose an issue in the crossbar that hangs the CPU on a module. As a result, a supervisor 2 module may report that a Generation 2 or Generation 3 module is not responding and then reload the module. This issue can occur in any of the following modules, on any MDS 9000 switch that supports these modules:

  - Cisco MDS 9000 4-Port 10-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 24-port 4-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module
  - Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)
  - Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16)

  Workaround: This issue is resolved.

- CSCtc22830

  Symptom: When you install and attempt to use a USB Flash drive on an MDS Supervisor 2 module, the support drives are not functional, but they do not report any useful information about they are not functional.

Workaround: This issue is resolved. NX-OS was enhanced to display a message such as the following: Please upgrade the Power Management EPLD to version 0xD or higher.

- CSCsh64824

  Symptom: When running FCIP compression, there is no easy way to see any flow control issues from the CLI or from Cisco Fabric Manager or Device Manager.

  Workaround: This issue is resolved. The CLI was enhanced to show ip compression flow control statistics.

- CSCsi33045

  Symptom: Dynamic port VSAN membership (DPVM) should provide list of ports that are up and that are preventing a DPVM session commit from succeeding.

  Workaround: This issue is resolved. DPVM has been enhanced to display detailed information when there is a DPVM activation failure. The information includes the list of switches that failed to activate and their IP address. The **show dpvm pending activation status** command displays the list of ports in an up state and that have a conflict in a VSAN.

- 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: This issue is resolved. The IF_DOWN_LINK_FAILURE message level is changed from 5 (notify) to 2 (critical).

- CSCtb80346

  Symptom: When and SFP is removed from a port that is administratively down or out of service, a message should be written to syslog or to the SNMP server that an SFP was removed.

  Workaround: This issue is resolved. Now when an SFP is removed, the following message is displayed: Interface <interface-id> is down (FCOT has been removed).

- CSCtc85276

  Symptom: When the MDS 9222i switch boots up, the ASCII configuration to provision an iSAPI application or feature on module 1 fails because the **install module 1 ssi <ssi-uri>** command is not supported on the MDS 9222i switch module 1. As a result, the iSAPI application or feature provisioning fails.

  Workaround: To reprovision the application or feature on the MDS 92221 switch module 1, follow these steps:

  1. Make sure that the SSI boot variable is set.
  2. Enter the **copy running-config startup-config** command to copy the running configuration to the startup configuration.
  3. Reload the MDS 9222i switch so that it boots up with the boot variable set to the SSI image.
  4. Provision the iSAPI application or feature.
  5. Enter the **copy running-config startup-config** command to copy the running configuration to the startup configuration. Be aware that this process is disruptive.

  Workaround: This issue is resolved for the MDS MSM-18/4 and MDS SSN-16 modules.

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.

- 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.

- CSCty32238

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

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

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

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

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

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

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

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

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

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

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

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
```

```
9    5.2(1)          1.0     22:01:00:0d:ec:25:e9:80 to 22:12:00:0d:ec:25:e9:80

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

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

Workaround: Upgrade to software release that has the fix for this issue.

- After performing a software upgrade to a Cisco NX-OS release that contains a fix for this issue, it may be necessary to enter the **shut** command followed by the **no shut** command on the affected host ports to regain connectivity.
- If you perform a nondisruptive upgrade or downgrade from a release that contains a fix to a release that does not contain the fix, you need to reload each module affected by this issue.
- If you have a Cisco MDS 9222i swtich that is affected by this issue, and you perform a nondisruptive upgrade or downgrade from a release that contains a fix to a release that does not contain the fix, you need to reload the switch.

- CSCsq20408

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

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

- CSCsy37951

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

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

- CSCtn68418

  Symptom: When you try to save a configuration, you might see the following message:

```
switch# copy run start
[########################################] 100%
Configuration update aborted: request was aborted
 %DAEMON-3-SYSTEM_MSG: ntp:can't open /mnt/pss/ntp.drift.TEMP: No space left on
device
- ntpd[xxxx]
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED
`show system internal flash` output will display /isan as 100% full.
Mount-on                 1K-blocks      Used   Available   Use%  Filesystem
```

```
/                         204800     54624      150176     27    /dev/root
/proc                          0         0           0      0    proc
/isan                     409600    409576          24    100    none
```

This symptom was seen because the Call Home feature had duplicate message throttling disabled and there were flapping interfaces that generated thousands of Call Home messages. These messages filled up the ISAN directory.

Workaround: To work around this issue, enable Call Home duplicate message throttling. If you find that the /isan directory is 100 percent full, open a TAC case to get assistance with deleting the files.

Related Documentation

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

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

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

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

Release Notes

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

Regulatory Compliance and Safety Information

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

Compatibility Information

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

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

Cisco NX-OS

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

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

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

Troubleshooting and Reference

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

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.