Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.0(1)

Release Date: April 17, 2006

Text Part Number: OL-8795-01 A1

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 48.

Note Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/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	04/17/2006	Created release notes
B0	04/19/2006	Added DDTS CSCsd92429.
C0	05/04/2006	Added DDTS CSCeg53114, CSCei79457, and CSCsd87853. Removed DDTS CSCeh22523, CSCei67982.
D0	05/22/2006	Added DDTS CSCsc20106, CSCsd89872, CSCsd94019, CSCsd94229, CSCsd97090, CSCse14087, CSCsd94718, CSCse12209, CSCse13769, and CSCse14032. Removed CSCeh52973. Revised the following sections: Upgrading, Reconfiguring SSM Ports, Migrating, Generation 2, Downgrading, and Limitations.

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

Table 1 Online History Change

Revision	Date	Description
E0	05/25/2006	Updated New Features and Limitations sections. Removed CSCse14087.
F0	06/23/2006	Added DDTS CSCsd95862, CSCsd19272, CSCse36768. Updated the New Features in Cisco MDS SAN-OS Release 3.0(1) section. Removed CSCeg33121, CSCeg12962, CSCeg84871, CSCeg90336, CSCeh04183, CSCeh30951, CSCeh70232, CSCeh93109, CSCei10774, CSCei36082, CSCei79457, CSCei53783, CSCsc46451, CSCsc95884, CSCec31365, CSCeg53114, CSCeg55238, CSCeh34828, CSCei48889,CSCei91676, CSCei91968, CSCej08751, CSCin92870, CSCin95789, and CSCsd71701.
G0	07/07/2006	Corrected the CWDM part numbers in Table 2.
H0	08//3/2006	Revised DDTS CSCsd89872 and CSCse84811
I0	08/18/2006	Added DDTS CSCse89151
J0	08/22/2006	Revised the Downgrading from Cisco MDS SAN-OS Release 3.0(1) section. Added DDTS CSCse65400.
K0	09/05/2006	Added DDTS CSCsd78967 and CSCse88606.
L0	09/7/2006	Added DDTS CSCec28084.
M0	09/13/2006	Added DDTS CSCsf21970.
N0	09/22/2006	Added the external crossbar module part number.
O0	11/29/2006	Added a note to the Downgrading section on having iSCSI enabled during a downgrade. Added a Limitation and Restriction about CWDM SFPs.
P0	11/30/2006	Added DDTS CSCin95789, CSCsd15794, CSCsd21187, CSCsd81137, CSCse22145, CSCse41442, CSCse70275, CSCse71420, CSCsf18552, CSCsf96043, CSCsf98427, CSCsg01963, CSCsg12020, and CSCsg15392.
Q0	12/07/2006	Added DDTS CSCsd99599.
R0	02/01/2007	Added DDTS CSCsg03171.
S0	02/22/2007	Added DDTS CSCsd92433, CSCsd97376, CSCse99087, CSCsg29400, CSCsg35972, CSCsg62359, CSCsg82792, CSCsh27840, and CSCsh31236.

Table 1 Online History Change

Revision	Date	Description
T0	04/04/2007	Added DDTS CSCsd41578 and CSCsh83200. Added the section "Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch". Added the section "Configuring Default Settings for the Default Zone".
U0	06/11/2007	Added DDTS CSCsh24256.
V0	07/18/2007	Removed DDTS CSCei82909.
W0	08/24/2007	Added DDTS CSCsd83775.
X0	10/23/2007	Removed DDTS CSCsh31236. Added information about Downgrading from Cisco SAN-OS Release 3.2(1) to the "Limitations and Restrictions" section.
Y0	04/30/2008	Added DDTS CSCso63465.
Z0	11/13/2008	Added the "Performing a Nondisruptive Software Upgrade on Generation 1 Modules" section.
A1	11/04/2010	Added the Supervisor-2A module to Table 2.

Contents

This document includes the following sections:

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.

The Cisco MDS 9000 Family SAN-OS is the underlying system software that powers the Cisco MDS 9500 series, 9200 series, and 9100 series multilayer switches. The Cisco SAN-OS provides intelligent networking features, such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 3.0(1) and includes the following topics:

Components Supported

Table 2 lists the software 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	M95S2K9-3.0.1	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.0.1	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-3.0.1	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-3.0.1	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series
	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with ASM or SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with ASM or SSM

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

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	MDS 9513 director (13-slot modular chassis with 11 slots for switching modules, and 2 slots reserved for Supervisor 2 modules only—SFPs[1] sold separately).	MDS 9513 only
	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 only
External crossbar module	DS-13SLT-FAB1	MDS 9513 Crossbar Fabric Module	MDS 9513 only
Supervisor modules	DS-X9530-SF2-K9	MDS 9500 Supervisor-2 module.	MDS 9500 Series only
	DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A module.	
	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I module.	

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

Component	Part Number	Description	Applicable Product
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
	DS-X9112	MDS 9000 12-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9124	MDS 9000 24-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9148	MDS 9000 48-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9200 Series, except for the MDS 9216
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage services module.	MDS 9500 Series and 9200 Series
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage services module.	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
Optics	DS-X2-FC10G-SR	X2/SC optics, 10-Gbps Fibre Channel for short wavelength mode.	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X2-FC10G-LR	X2/SC optics, 10-Gbps Fibre Channel for long wavelength mode.	
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW[2]	2-Gbps/1-Gbps Fibre Channel—short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW[2]	2-Gbps/1-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-FCGE-SW[2]	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW[2]	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-GE-T[2]	1-Gbps Ethernet SFP.	
	DS-SFP-FC4G-SW[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—short wavelength SFP for DS-X91xx switching modules.	
	DS-SFP-FC4G-MR[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 4 km.	
	DS-SFP-FC4G-LW[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 10 km.	

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

Component	Part Number	Description	Applicable Product
CWDM[4]	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexers.	
Power supplies	DS-CAC-6000W	6000-W AC power supply.	MDS 9513 only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-3000W	3000-W AC power supply	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-300W	300-W[5] AC power supply.	MDS 9100 Series only
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512 MB.	MDS 9500 Series only
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
CD-ROM	M90FM-CD-212=	MDS 9000 Management Software and Documentation CD-ROM, spare.	MDS 9000 Family

1. SFP = small form-factor pluggable
2. Supported on the DS-X9530-SF1-K9, MDS 9500 Series Supervisor module only
3. Supported on the DS-X9530-SF2-K9, MDS 9500 Series Supervisor-2 module only
4. CWDM = coarse wavelength division multiplexing
5. W = Watt

Determining the Software Version

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

To determine the version of Cisco MDS 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 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.

Downloading Software

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

http://www.cisco.com/public/sw-center

Upgrading Your Cisco MDS SAN-OS Software Image

The Cisco MDS SAN-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.

Use the following guidelines to nondisruptively upgrade your Cisco MDS SAN-OS Release 3.0(1):

- Install and configure dual supervisor modules.
- 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 SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
- Follow the upgrade path for your current release:
  - Upgrading from Cisco SAN-OS Release 1.x to Release 3.x requires that you upgrade first to Cisco SAN-OS Release 1.3(4a), then upgrade to Cisco SAN-OS Release 2.1(2b), then upgrade to Cisco SAN-OS Release 3.0(1).
  - Upgrading from Cisco SAN-OS Release 2.0(2b), 2.0(2c), 2.0(3), 2.1(2b), 2.1(2c), 2.1(2d), and 2.1(2e), allows you to nondisruptively upgrade directly to Release 3.0(1). If you do not have one of these releases installed, you must upgrade first to Cisco SAN-OS Release 2.1(2b) and then upgrade to Cisco SAN-OS Release 3.0(1).
  - Upgrading from Cisco SAN-OS Release 2.x releases to Release 3.x requires that you upgrade first to Cisco SAN-OS Release 2.1(2b) and then upgrade to Cisco SAN-OS Release 3.0(1).
  - If you have IVR enabled and you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or Release 2.1.(2a), there are additional steps you should follow before upgrading. See *"Upgrading with IVR Enabled" section on page 11*.
  - Upgrading for FICON from Cisco SAN-OS Release 1.x to Release 3.x requires that you upgrade first to Cisco SAN-OS Release 1.3(4a), then upgrade to Cisco SAN-OS Release 2.0(2b), then upgrade to Cisco SAN-OS Release 3.0(1).
- All Gigabit Ethernet ports are disruptive on upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. This impacts those nodes that are members of VSANs traversing an FCIP ISL and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
- Layer 3 switching on SSM ports are disruptive on upgrades or downgrades. Layer 2 switching can be nondisruptive 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 SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
  - All SMM applications are disabled. Use the **show ssm provisioning** CLI command to determine what applications are configured. Use the **no ssm enable feature** CLI command to disable these applications.
  - No SSM ports are in auto mode. See *Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(1), page 13*.

  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** CLI 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 MDS Storage Services Module Interoperability Support Matrix* and the *Managing Modules* chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x,* for information on upgrading your SSM.
- Use the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- If you are using FCIP tape acceleration and you are upgrading from Cisco MDS SAN-OS Release 2.x to Release 3.x, you should disable the FCIP tape acceleration feature prior to the upgrade. After the upgrade, you should re-enable FCIP tape acceleration.

Caution Upgrading to Cisco MDS SAN-OS Release 2.1(2) or later from any release can disrupt traffic on any SSM installed on your MDS switch.

Note Upgrading from Cisco MDS SAN-OS Release 1.x directly to Cisco SAN-OS Release 3.x is disruptive to all Fibre Channel and Gigabit Ethernet ports.

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

Performing a Nondisruptive Software Upgrade on Generation 1 Modules

Generation 1 modules may reload during a nondisruptive SAN-OS software upgrade because of the CompactFlash being unable to partition for the new code. If that happens, the installer aborts and reloads the module.

This issue affects the following modules:

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

This issue might be seen during an upgrade from Cisco SAN-OS Release 3.0(x), 3.1(x) or 3.2(x). It has been addressed for upgrades from SAN-OS Release 3.3(1) or higher. Therefore, you will not be impacted by this issue if you are running SAN-OS Release 3.3(1) when you upgrade to a higher SAN-OS release.

When this problem occurs, the module will automatically reload and may cause the Install All to stop, which will cause the upgrade to be unsuccessful. Error messages similar to the following may be displayed:

```
Install has failed. Return code 0x40930020 (Non-disruptive upgrade of a module failed).
Please identify the cause of the failure, and try 'install all' again.
Module 2: Non-disruptive upgrading.
-- FAIL. Return code 0x40690009 (Error in downloading image for image upgrade).
```

To avoid this kind of unplanned disruption, follow the methods for identifying and correcting this issue described in Cisco Field Notice 63099, before proceeding with the SAN-OS upgrade.

This Field notice can be found under the Support, Products page for Cisco MDS9500 Series Multilayer Directors selection.

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 running might be disruptive. Some possible scenarios include:

- 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 RDI failure and the flapped lSL could remain in a down state because of a domain overlap. This is caused by conflicts between the allowed domains list and the virtual domain requested through RDI.

This issue was resolved in an earlier release, however upgrades from Cisco SAN-OS Release 2.1(1a), 2.1(1b), or 2.1(2a) to Release 3.0(1) when IVR is enabled requires that you use the following workaround.

For VSANS in interop mode 2 or 3, issue an IVR refresh, and then follow the upgrade guidelines listed in "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 9.

To upgrade from Cisco SAN-OS Release 2.1(1a), 2.1(1b), or 2.1(2a) to Release 3.0(1) 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 1-4093** command to disable RDI mode on all IVR enabled switches. 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.

Example Syslog Error Messages

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
port-channel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface port-channel 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 3.0(1) in "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 9.

If you are adding new switches running Cisco MDS SAN-OS Release 3.0(x), upgrade all your existing switches to Release 3.0(1) as described in this procedure. Then add new switches.

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

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 3.

Table 3 Software Image for Supervisor Type

Supervisor Type	Switch	Image
Supervisor-1 module	MDS 9506 and 9509	Filename begins with m9500-sf1ek9
Supervisor-2 module	MDS 9506, 9509, and 9513	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch.

For a Supervisor-1 module, the output might look like this:

```
switch# show module
Mod  Ports  Module-Type                        Model               Status
---  -----  -------------------------------- ------------------ ------------
...
...
5    0      Supervisor/Fabric-1               DS-X9530-SF1-K9    active*
6    0      Supervisor/Fabric-1               DS-X9530-SF1-K9    ha-standby
```

For a Supervisor-2 module, the output might look like this:

```
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
```

Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(1)

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode. Because auto mode is the default for releases prior to Release 3.0(1), you should modify the configuration of the ports before upgrading a SAN-OS software image prior to Release 3.0(1) to avoid any traffic disruption.

For more information on upgrading SAN-OS software, see "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 9.

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 might cause a disruption if the port is currently operating in E mode.

To make the configuration change 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 Fx if the current operational port mode is 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. If the admin port mode of these ports is auto or E, change the admin port mode to Fx.

```
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
```

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

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

Caution Migrating your supervisor modules is a disruptive operation.

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

To migrate from a Supervisor-1 module to a Supervisor-2 module, refer to the step-by-step instructions in the *Cisco MDS 9000 Family CLI Configuration Guide*.

Configuring Generation 2 Switching Modules

The Cisco MDS 9500 Multilayer Directors are designed to operate with any combination of Cisco MDS 9000 Generation 1 and Generation 2 modules. However, there are limitations to consider when combining the various modules and supervisors in the Cisco MDS 9500 Series platform chassis. The references listed in this section provide specific information about configurations that combine different modules and supervisors.

For information on configuring Generation 2 switching modules, refer to:

http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664c6b.html

For information on port index availability, refer to:

http://www.cisco.com/en/US/products/ps5990/products_installation_guide_chapter09186a0080419599.html

For information on Cisco MDS 9000 hardware and software compatibility, refer to:

http://www.cisco.com/en/US/products/ps5989/products_device_support_table09186a00805037ee.html

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

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

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

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path listed inthis section, 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(2b) to SAN-OS Release 3.0(1)), 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.

New Features in Cisco MDS SAN-OS Release 3.0(1)

This section lists the new software features in Cisco MDS SAN-OS Release 3.0(1).

FCIP Tape Read Acceleration

Tape drives can have one read I/O command outstanding at a time, which means that increased latency significantly impacts tape read performance. The Fibre Channel over IP (FCIP) tape read acceleration feature improves tape restore operation performance by reading ahead and buffering tape data on the switch. Subsequent tape reads are not impacted by the WAN link latency because the read ahead data is buffered at the switch closest to the host requesting the data.

Fabric Binding for Fibre Channel

Fabric binding ensures Inter-Switch Links (ISLs) are only enabled between specified switches in the fabric binding configuration. Cisco MDS SAN-OS 3.0(1) supports fabric binding for Fibre Channel VSANs as well as FICON VSANs.

FICON Port Swapping Enhancement

Provides the ability to port swap using the interface identifier when there are duplicate port numbers on a switch.

Generation 2 Switching Module Support

The Cisco MDS 9500 Series of switches support the following set of modules called Generation 2 modules.

- DS-X9148 MDS 9000, 48-port 4-Gbps Fibre Channel module.
- DS-X9124 MDS 9000, 24-port 4-Gbps Fibre Channel module.
- DS-X9112 MDS 9000, 12-port 4-Gbps Fibre Channel module.
- DS-X9704 MDS 9000, 4-port 10-Gbps Fibre Channel module.

Detailed information about configuring the new Generation 2 Fibre Channel switching modules is available in the *Cisco MDS 9000 Family CLI Configuration Guide* and the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

IKE Digital Certificates

The IP security (IPsec) protocol uses the Internet Key Exchange (IKE) protocol to handle protocol and algorithm negotiation and to generate the encryption and authentication keys to be used by IPsec. While IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys. IKE uses RFCs 2408, 2409, 2410, and 2412, and implements the draft-ietf-ipsec-ikev2-16.txt draft.

IKE Fully Qualified Domain Names

IKE for IPsec has been enhanced to allow users to enter fully qualified domain names instead of IP addresses.

IKE Host Name Support

An IKE identity host name can be specified instead of an IP address for preshared keys.

IPsec Authentication Enhancements

Certificate Authorities (CAs) manage certificate requests and issue certificates to participating IPsec network devices. When a new device attempts an IPsec connection, certificates are automatically exchanged and the device can be authenticated. Although IPsec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPsec.

IVR Enhancements

Inter-VSAN Routing (IVR) enhancements include the following:

- IVR Service Groups—You can have more than one active IVR service group.
- IVR Zone Renaming—You can rename IVR zones.
- IVR Zone Set Renaming—You can rename IVR zone sets.
- Active IVR Zone Set Copy—You can copy the IVR active zone set to the full IVR zone set to be edited and reactivated.
- Active IVR Topology Copy—You can copy the IVR active topology to the manually configured IVR topology.

FICON Port Numbering

A range of 255 port numbers are available for you to assign to all the ports on a switch. However, you can have more than 255 physical ports on a switch and the excess ports do not have port numbers in the default numbering scheme. When you have more than 255 physical ports on your switch, you can assign unimplemented port numbers (those that are not assigned by default to a slot in the chassis) to the ports, or assign duplicate port numbers if they are not used in the same FICON VSAN.

iSCSI Server Load Balancing (iSLB)

The iSCSI server load balancing (iSLB) feature provides a means to easily configure large scale iSCSI deployments containing hundreds or even thousands of initiators. iSLB provides the following features:

- The iSLB initiator configuration is simplified with support for initiator targets and auto-zones.
- Cisco Fabric Services (CFS) eliminates the need for manual configuration by distributing the iSLB initiator configuration among all MDS switches in the fabric.
- There is dynamic load balancing of iSLB initiators using iSCSI login redirect and VRRP.

iSNS Cloud Discovery

The Internet storage name service (iSNS) cloud discovery feature provides information to the iSNS server on the various interfaces reachable from an initiator by partitioning the interfaces on a switch into disjointed IP clouds. This discovery is achieved by sending messages to all other known IPS ports that are currently up and, depending on the response (or the lack of it), determines if the remote IPS port is in the same IP network or in a different IP network.

The iSNS server distributes cloud and membership information across all the switches using CFS. Therefore, the cloud membership view is the same on all the switches in the fabric.

IPv6

IP version 6 (IPv6) provides extended addressing capability beyond those provided in IP version 4 (IPv4) in Cisco MDS SAN-OS. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses. IPv6 provides the following enhancements over IPv4:

- Allows networks to scale and provide global reachability.
- Handles packets more efficiently because the IPv6 packet header format is simplified.
- Reduces the need for private address and network address translation (NAT).
- Provides simpler autoconfiguration of addresses.

IPv6 Access Control Lists (IPv6-ACLs)

IP version 6 access control lists (IPv6-ACLs) provide basic network security to all switches in the Cisco MDS 9000 Family. IPv6-ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

Each switch in the Cisco MDS 9000 Family can have a maximum of 64 IPv6-ACLs and each IPv6-ACL can have a maximum of 256 filters.

CFS Over IP Distribution

Starting with SAN-OS Release 3.0(1), CFS can distribute application data over IP connections. Distribution over IP is transparent to the application, but the application must register with CFS for the application data to be distributed over IP. The following CFS applications register for the CFS-over-IP distribution option: NTP, role, RADIUS, TACACS+, syslogd, and Call Home.

CFS Support for Allowed Domain ID Lists

Allowed domain ID lists can be distributed in the fabric using the CFS infrastructure. There are two obvious benefits:

- Users can save time because they no longer have to enter the same **fcdomain** command on every switch in a VSAN to configure allowed domains. Instead, users can enter the command once and commit it across the entire fabric.
- Users are less likely to make typing mistakes or to forget to configure a switch—two common mistakes caused by repeated typing of the same command. With CFS, users are guaranteed that the same list of allowed domains is distributed to all switches in the fabric or to no switches in the fabric.

In-Order Delivery Enhancements

In-order delivery (IOD) of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator. If the in-order guarantee feature is enabled, frames are delivered in order within the switch latency drop period. The in-order delivery feature can be enabled for a specific VSAN or for the entire switch.

CLI Enhancements

The Cisco MDS SAN-OS command-line interface (CLI) has been enhanced to support:

- Command variables. You can define variables that persist for the duration of a session or across sessions and switch reloads.
- Common command aliases. You can define command aliases that are global for all user sessions and that persist across reboots.

AAA Server Enhancements

Because an unresponsive AAA server introduces delay in processing of AAA requests, an MDS switch can periodically monitor an AAA server to check whether it is responding (or alive) to save time in processing AAA requests. The MDS switch marks unresponsive AAA servers as dead and does not send AAA requests to any dead AAA servers. An MDS switch periodically monitors dead AAA servers and brings them to the alive state once they are responding. This monitoring process verifies that an AAA server is in a working state before real AAA requests are sent its way. Whenever an AAA server changes to the dead or alive state, an SNMP trap is generated and the MDS switch warns the administrator that a failure is taking place before it can impact performance.

SSH Authentication Enhancements

SSH authentication on the Cisco MDS 9000 Family switches provides X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that vouches for the origin and integrity of a message. It contains encryption keys for secured communications and is “signed” by a trusted certificate authority (CA) to verify the identity of the presenter. You can configure your switch for either SSH authentication using an X.509 certificate or SSH authentication using a public key certificate, but not both.

Call Home Enhancements

A Call Home alert group can be customized with user-defined **show** commands whose output can be attached to a Call Home message being sent. Five commands can be specified per alert group.

Online Health Management System Enhancements

The online health management system (OHMS) has been enhanced to provide increased system health capabilities through new loopback testing features. OHMS also includes support for on-board failure logging (OBFL) for Generation 2 modules and loopback enhancements.

McDATA Native Interoperability

Release 3.0(1) includes commands to configure McDATA native mode interoperability.

Increased Zone Limit per VSAN

The maximum number of zones per VSAN has increased from 2000 to 8000. The maximum number of zones in the fabric is 8000.

MS-CHAP

The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) can be used for user logins to an MDS switch through a remote authentication server (RADIUS or TACACS+). MS-CHAP must be explicitly enabled to be used.

boot auto-copy Command Enabled by Default

The **boot auto-copy** command is enabled by default.

N-Port Identifier Virtualization

N-port identifier virtualization (NPIV) provides a means to assign multiple port IDs to a single N port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level. NPIV must be globally enabled for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port FC IDs.

RSCN Timer Configuration

The Registered State Change Notification (RSCN) timer value can be configured per VSAN, and must be the same on all switches in the VSAN. Because the time-out value for each switch is configured manually, a misconfiguration occurs when different switches time out at different times. This misconfiguration means that different N ports in a network can receive RSCNs at different times. The Cisco Fabric Services (CFS) infrastructure alleviates this situation by automatically distributing the RSCN timer configuration information to all switches in a fabric.

Modem Support for Supervisor-2 Modules

There is new information available for configuring modem parameters on Supervisor-2 modules.

Configuration Check

The **show incompatibility system** command has been modified to indicate the commands to use to disable features before downgrading to an earlier system image.

SMI-S 1.1.0 Support

The Cisco MDS SAN-OS Release 3.0(1) embedded CIM agent is compliant with SMI-S version 1.1.0. The new CIM agent includes a new access point profile.

New SAN-OS MIBs

The following new Management Information Base (MIBs) are available for Cisco MDS SAN-OS Release 3.0(1):

- CISCO-COMMON-MGMT-MIB
- CISCO-IETF-VRRP-MIB
- CISCO-PKI-PARTICIPATION-MIB

Note If you use the CISCO-FICON-MIB, be aware that the MODULE-IDENTITY value has changed in Cisco MDS SAN-OS Release 3.0(1) to CiscoMgmt 375. In SAN-OS Release 2.0(1a) through Release 2.2(1f), the value of MODULE-IDENTITY was CiscoMgmt 88888.

SFP Diagnostic Information

Diagnostic information from small form-factor pluggable (SFP) optical transceivers is supported on the following Cisco MDS 9000 Fibre Channels switching modules:

- 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 4-port 10-Gbps Fibre Channel switching module

The SFP diagnostic information enables you to quickly isolate physical layer problems, like contact problems, major failures within SFPs, or abnormal error rates associated with excessive optical attenuation. The following information is provided:

- Temperature
- Voltage and current
- Transmit power level
- Receive power level

Crossbar Management

The Cisco MDS 9500 Series Directors running Cisco MDS SAN-OS Release 3.0(1) or later support the following types of crossbars:

- Integrated crossbar—Located on the Supervisor 1 and Supervisor 2 modules. The Cisco MDS 9506 and 9509 Directors only use integrated crossbars.
- External crossbar—Located on an external crossbar switching module. External crossbar switching modules are required for Cisco MDS 9513 Directors.

You can mix and match Generation 1 and Generation 2 hardware on the Cisco MDS 9500 Series Directors running Cisco MDS SAN-OS Release 3.0(1) or later without compromising the integrity and availability of your SANs based on Cisco MDS 9500 Series Directors. However, to realize these benefits, there are several important operational requirements that you must consider when *removing* crossbars for maintenance activities. For information about these operational requirements, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and the *Cisco MDS 9500 Series Hardware Installation Guide*.

Fabric Manager Server Enhancements

This section lists the additional enhancements that are available through the the Fabric Manager Server, but not through the command-line interface.

Performance Prediction Trending

A Performance Prediction report in Fabric Manager Server allows you to more reliably predict when storage network connections will become over utilized. You can define the time horizon for the analysis in 3-, 6-, or 12- month intervals and the threshold level. Fabric Manager Server extrapolates the performance and lists in chronological order those interfaces that are expected to reach the threshold level in the specified time horizon.

Configurable RRD

Fabric Manager Server historical performance statistics are stored in a round-robin database (RRD) that holds up to one year of statistics. Performance statistics are rolled up progressively as the data ages to reduce the storage space requirements. The number of samples saved for each resolution can be configured, which allows you to manage the resolution and time period for the Fabric Manager Server historical performance statistics.

Custom Report Performance Chart

Custom reports allow users to optionally embed throughput performance charts for each table entry. If errors or discards are not zero, charts are also included for those statistics.

Server Performance Summary Report

This report allows users to view summary throughput, errors, and discard statistics for all connections on paths from a server to its storage devices, which makes it possible to rapidly pinpoint connectivity problems. The Server Performance Summary Report includes statistics for relevant connections from the server to switch, Inter-Switch Links (ISLs), and switch to storage connections in the paths.

Data Collection Auto-Update

The data collection auto-update feature eliminates most of the manual effort of keeping the Performance Manager data collection configuration up-to-date. Performance data can be collected on all host connections, storage connections, ISLs, and flows. As new host connections, storage connections, or ISLs are added, Fabric Manager Server automatically updates the data collector configuration to include them. Fabric Manager Server also updates the data collection configuration to add Fibre Channel flows, but the new flows must first be created.

Event Forwarding

Events logged by Fabric Manager Server can be forwarded to users through e-mail. All events within specific fabrics or VSANs that are at or above a user-selected severity level are forwarded. Multiple destinations can be configured to receive the e-mail. In addition, users can be paged by sending the e-mail to a paging gateway.

Filtering by User-Defined Groups

You can now define custom groups that contain switches, hosts, or storage devices. These groups filter out information that is not relevant to the group on the Cisco Fabric Manager topology map, in information tables (switch parameters), and in Fabric Manager Server reports. These groups supplement the existing user-defined grouping capabilities for creating host or storage enclosures.

SNMP over TCP/IP

SNMP messages can be transported over TCP rather than UDP for management traffic on the out-of-band Gigabit Ethernet management port (mgmt0).

EMC Call Home

Traps can be forwarded as XML data using e-mail, according to EMC specifications.

New Hardware Features

This section lists the new hardware supported by Cisco MDS SAN-OS Release 3.0(1).

Cisco MDS 9513 Director

The Cisco MDS 9513 Director is a 13-slot Fibre Channel switch. The front panel consists of 13 horizontal slots, where slots 1 to 6 and slots 9 to 13 are reserved for switching and services modules only, and slots 7 and 8 are for Supervisor-2 modules only. A variable speed fan tray, with 15 individual fans, is located on the front left panel of the chassis.

Cisco MDS 9500 Series Supervisor-2 Module

The Cisco MDS 9500 Series offers redundant, hot-swappable, Supervisor-2 modules that can be used in slots 5 and 6 of the Cisco MDS 9509 and 9506 Directors. Dual Supervisor-2 modules must be used in slots 7 and 8 of the Cisco MDS 9513 Director.

Supervisor-2 modules provide a crossbar switching fabric to connect all the switching modules. Single fabric configurations provide 720-Gbps full duplex speed with 80-Gbps full duplex bandwidth per switching module. Dual fabric configurations provide 1.4-Gbps speed with 160-Gbps full duplex

bandwidth per switching module. This crossbar switching fabric is disabled when a Supervisor-2 module is installed in a Cisco MDS 9513 Director. The Cisco MDS 9513 Director supports two crossbar switching modules located at the rear of the chassis that handle this function.

For detailed information about migrating from Supervisor-1 to Supervisor-2 modules, refer to the *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide.*

Cisco MDS 9000 48-Port 4-Gbps Fibre Channel Switching Module

The 48-port 4-Gbps Fibre Channel switching module offers 48 autosensing 1-, 2-, and 4-Gbps Fibre Channel ports and can be used in any Cisco MDS 9500 Series chassis and in the Cisco MDS 9216i and 9216A switches. The 48-port switching module can be configured in one of two operational modes: shared bandwidth mode (default), and dedicated bandwidth mode.

Cisco MDS 9000 24-Port 4-Gbps Fibre Channel Switching Module

The 24-port 4-Gbps Fibre Channel switching module offers 24 autosensing 1-, 2-, and 4-Gbps Fibre Channel ports and can be used in any Cisco MDS 9500 Series chassis and in the Cisco MDS 9216i and 9216A switches. The 24-port switching module can be configured in one of two operational modes: shared bandwidth mode (default), and dedicated bandwidth mode.

Cisco MDS 9000 12-Port 4-Gbps Fibre Channel Switching Module

The 12-port 4-Gbps Fibre Channel switching module can be used in any Cisco MDS 9500 Series chassis and in the Cisco MDS 9216i and 9216A switches. The switching module is a full rate mode module providing 12 SPF-based Fibre Channel interfaces. Each interface is capable of supporting full line rate operation at 4-Gbps interface speed. The module delivers a sustained data rate of up to 4-Gbps in each direction, on all ports simultaneously and up to 96 Gbps of continuous, aggregate bandwidth when attached to high performance servers and storage subsystems.

Cisco MDS 9000 4-Port 10-Gbps Fibre Channel Switching Module

The 4-port 10-Gbps Fibre Channel switching module offers four dedicated bandwidth Fibre Channel ports running at 10 Gbps with no oversubscription. This module can be used in any Cisco MDS 9500 Series chassis and in the Cisco MDS 9216i and 9216A switches. The module delivers a sustained data rate of up to 10 Gbps in each direction, on all ports simultaneously, and up to 80 Gbps of continuous, aggregate bandwidth when attached to high performance servers and storage subsystems.

Crossbar Module

The Cisco MDS 9513 Director supports two crossbar switching modules located at the rear of the chassis. Each Supervisor-2 module has an associated crossbar switching module. Redundant crossbar switching modules act in an active-active method, where each switching module forwards traffic across both crossbar fabrics based on the intended destination. Therefore the traffic load is shared across both crossbar switching modules. Each crossbar fabric channel connects to a fabric interface ASIC on the

switching modules through serial links on the midplane. Each Supervisor-2 module processor also has a 20-Gbps (40-Gbps FDX) link to each crossbar fabric for participating in management and control protocols and for in-band diagnostics.

X2 Transceiver

The 4-port 10-Gbps Fibre Channel switching module provide four dedicated bandwidth Fibre Channel ports that support standard modular X2 transceiver interfaces at the fixed speed of 10 Gbps.

Gigabit Ethernet SFP Transceiver

The 4-port and 8-port IP Storage services (IPS-4 and IPS-8) modules provide four or eight 1-Gigabit Ethernet ports that support Gigabit Ethernet SFP transceivers. The Gigabit Ethernet SFP transceivers have RJ-45 connectors and support Gigabit Ethernet (1 Gbps).

Limitations and Restrictions

This section lists the limitations and restrictions for this release.

Reconfiguring SSM Ports

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). For instructions about how to modify the configuration of the ports before upgrading to SAN-OS Release 3.0(1), see the "Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(1)" section on page 13.

Downgrading from Cisco MDS SAN-OS Release 3.0(1)

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.0(1):

- Install and configure dual supervisor modules.
- 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*.
- Disable all features not supported by the downgrade release. Us the **show incompatibility system** *downgrade-image* CLI command to determine what you need to disable.
- Follow the downgrade path for your current release:
  - Downgrading to Cisco SAN-OS Release 1.x from Release 3.x requires that you downgrade first to Cisco SAN-OS Release 2.1(2b), then downgrade to Cisco SAN-OS Release 1.3(4a), then downgrade to your 1.x release.
  - You can downgrade nondisruptively from 3.x to the following releases:2.0(2b), 2.0(2c), 2.0(3), 2.1(2b), 2.1(2c), 2.1(2d), 2.1(2e), and 3.0(1). Downgrading to other Cisco SAN-OS Release 2.x releases from Release 3.x requires that you downgrade first to Cisco SAN-OS Release 2.1(2b) and then downgrade to an earlier 2.x release.

  - Downgrading for FICON to Cisco SAN-OS Release 1.x from Release 3.x requires that you downgrade first to Cisco SAN-OS Release 2.0(2b), then downgrade Cisco SAN-OS Release 1.3(4a), and then downgrade to your 1.x release.
- All Gigabit Ethernet ports are disruptive on upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. This impacts those nodes that are members of VSANs traversing an FCIP ISL or iSCSI initiators connected to the Gigabit Ethernet ports.
- Enable iSCSI if an IPS module or a MPS-14/2 module is online in the switch. Otherwise, the downgrade will disrupt traffic.
- Layer 3 switching on SSM ports are disruptive on upgrades or downgrades.
- Layer 2 switching on SSM ports can be nondisruptive under the following conditions:
  - All SMM applications are disabled. Use the **show ssm provisioning** CLI command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** CLI command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** CLI command to determine your EPLD version. Refer to *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco MDS Storage Services Module Interoperability Support Matrix* and to the *Managing Modules* chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x* for information on downgrading your SSM.
- Layer 2 switching traffic is not disrupted when downgrading to Cisco SAN-OS Release 2.1(2) or later.

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

Downgrading from Cisco SAN-OS Release 3.2(1)

Following a downgrade from Cisco MDS SAN-OS Release 3.2(1) to an earlier SAN-OS release that does not support the Data Mobility Manager (DMM) feature that is offered from SAN-OS Release 3.2(1) onwards, you might have stale configuration information on the switch, if you had provisioned DMM on the SSM. In this situation, you can remove the stale configuration from the SSM by entering the following commands:

```
switch(config)#  poweroff module slot
switch# purge module slot running-config
```

ISNS Server

The iSCSI ISNS server feature is not supported in Cisco MDS SAN-OS Release 3.0(1).

CWDM SFPs

Some 2-Gbps CWDM SFPs do not have have speed capability encoded in EEPROM memory and they could negotiate and obtain synchronization up to 4-Gbps on modules that support 4-Gbps speed. As a result, the link comes up and appears to work, but then becomes disabled and connectivity problems occur. To correct this problem, both sides of the connection must have their speed fixed to 1- or 2-Gbps instead of Auto.

10-Gbps Inter-Switch Links

- **Graceful Shut Down and Bring Up of 10-Gbps ISL Links:** For all planned 10-Gbps Inter-Switch Link (ISL) outages, it is mandatory that you perform those operations using either the **shutdown** and **no shutdown** commands from the CLI, or the Port Disable and Port Enable feature in Cisco Fabric Manager. If any unplanned outages occur, such as when the ISL cable or X2 transceiver with the ISL cable is unplugged, you should still shut down the 10-Gbps interface from the CLI or Fabric Manager. Once you plug in the ISL cable, bring up the10-Gbps interface using the CLI or Fabric Manager.
- The extended buffer-to-buffer credits (BB_credits) feature is currently not supported on 10-Gbps ISLs.

These restrictions will be addressed in a future Cisco SAN-OS software release.

Configuring Default Settings for the Default Zone

Following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release, the configuration defined by the **zone default-zone permit vsan** *vsan-id* command is applied only to the active VSAN. The configuration does not apply to unconfigured VSANs. In SAN-OS 3.x, you can apply the configuration to unconfigured VSANs by issuing the **system default zone default-zone permit** command.

Similarly, the **zoneset distribute full vsan** *vsan-id* command applies only to the active VSAN following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release.

Although you can configure the default-zone settings in the setup script, these settings do not take effect for VSAN 1, because VSAN 1 already exits prior to running the setup script. To configure the default settings for the default-zone in VSAN 1, you must explicitly enter the **zone default-zone permit** command.

Caveats

This section lists the open and resolved caveats for this release. Use Table 4 to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 4 Open Caveats and Resolved Caveats Reference

	Software Release (Open or Resolved)	
DDTS Number	**2.1(2e)**	**3.0(1)**
Severity 2		
CSCeh73149	O	R
CSCeh92604	O	R
CSCei18830	O	R
CSCei19822	O	R
CSCec28084	–	O
CSCsc45880	–	O
CSCsc75056	O	R

Table 4 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.1(2e)	3.0(1)
CSCsc76467	O	R
CSCsd19272	O	O
CSCsd41578	O	R
CSCsd45429	O	R
CSCsd47064	O	O
CSCsd78967	O	R
CSCsd79954	O	R
CSCsd94229	–	O
CSCsd95862	O	O
CSCsd97090	–	O
CSCsd97376	–	O
CSCse65400	O	O
CSCse89151	O	R
CSCsf98427	–	O
CSCsg01963	–	O
CSCsg35972	–	O
CSCsh27840	O	O
Severity 3		
CSCef56229	O	R
CSCeg27584	O	R
CSCeh33548	O	R
CSCeh41099	O	R
CSCeh75500	O	R
CSCeh88814	O	R
CSCei32317	O	R
CSCei57342	O	R
CSCei58652	O	R
CSCei71686	O	R
CSCei86399	O	R
CSCei91968	O	R
CSCej08751	O	R
CSCin95686	O	R
CSCin95789	O	O
CSCsb89732	O	R
CSCsc09732	O	R

Table 4 Open Caveats and Resolved Caveats Reference (continued)

	Software Release (Open or Resolved)	
DDTS Number	**2.1(2e)**	**3.0(1)**
CSCsc20106	O	O
CSCsc28722	O	R
CSCsc31424	O	R
CSCsc33788	O	R
CSCsc40012	O	R
CSCsc48919	O	R
CSCsc60283	O	R
CSCsc72994	O	R
CSCsc93936	O	R
CSCsc95657	–	O
CSCsc97070	O	R
CSCsd02008	O	R
CSCsd07246	O	R
CSCsd12831	O	R
CSCsd15794	O	O
CSCsd21187	O	O
CSCsd22920	O	R
CSCsd25790	O	R
CSCsd30165	O	R
CSCsd34882	O	O
CSCsd51194	–	O
CSCsd52037	–	O
CSCsd53429	O	R
CSCsd58774	O	R
CSCsd60578	O	R
CSCsd70927	O	R
CSCsd72822	O	R
CSCsd73494	O	R
CSCsd75284	O	R
CSCsd76429	O	R
CSCsd79575	–	O
CSCsd79938	O	O
CSCsd81137	O	O
CSCsd81725	O	R
CSCsd82449	O	R

Table 4 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.1(2e)	3.0(1)
CSCsd83775	O	R
CSCsd87853	–	O
CSCsd89872	O	O
CSCsd92429	O	R
CSCsd93011	O	R
CSCsd94019	O	O
CSCsd94718	O	O
CSCsd99599	–	O
CSCse12209	–	O
CSCse13769	–	O
CSCse14032	O	O
CSCse22145	O	O
CSCse36768	–	O
CSCse41442	O	O
CSCse70275	O	O
CSCse71420	O	O
CSCse84811	O	O
CSCse88606	O	O
CSCse99087	O	O
CSCsf18552	–	O
CSCsf96043	O	O
CSCsf21970	O	R
CSCsg03171	O	O
CSCsg12020	O	O
CSCsg15392	O	O
CSCsg29400	–	O
CSCsg62359	O	O
CSCsg82792	–	O
CSCsh24256	–	O
CSCsh83200	–	O
CSCso63465	O	O
Severity 4		
CSCsd70102	O	R
CSCsd85503	–	O

Table 4 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.1(2e)	3.0(1)
Severity 6		
CSCsd92433	O	O

Resolved Caveats

- CSCeh73149

  Symptom: If you perform a suspend/resume operation on a SANTap target VSAN, I/O timeout may occur for some of the LUNs on the target.

  Workaround: None. This issue has been resolved.

- CSCeh92604

  Symptom: Enabling IVR NAT on the same switch where write acceleration is enabled over a PortChannel with multiple FCIP links may result in frames not transferring from the source to the destination unless a transit VSAN spanning the FCIP PortChannel is configured.

  Note The resolution of this issue *requires* that you configure a transit VSAN spanning the FCIP PortChannel. In the following example, the FCIP port channel is in IVR transit VSAN 3.

  ```
  Host --- VSAN 1 --- MDS --- FCIP PortChannel in VSAN 3 --- MDS --- VSAN 2 --- Disk
  ```

  Workaround: None. This issue has been resolved.

- CSCei18830

  Symptom: Removing zones from an active zone set may generate a system message that the zone activation has failed because of an Accept Change Authorization (ACA) failure.

  Workaround: None. This issue has been resolved.

- CSCei19822

  Symptom: An active IVR zone set on the local switch is not propagated when the commit session contains any other configuration changes.

  Workaround: None. This issue has been resolved.

- CSCsc75056

  Symptom: Installing an invalid license file may cause an MDS switch to reload.

  Workaround: None. This issue has been resolved.

- CSCsc76467

  Symptom: The IPFC manager fails when it receives an FARP packet for a nonexistent VSAN interface. This situation may occur when a host bus adapter (HBA) on a host directly registers as an IPFC interface.

  Workaround: None. This issue has been resolved.

- CSCsd41578

  Symptom: When a port continuously flaps, the Fibre Channel Name Server may crash and cause a supervisor switchover.

Workaround: None. This issue is resolved.

- CSCsd79954

  Symptom: A VSAN that is connected to a McDATA switch with interop mode 1 participates in IVR. The VSAN has devices that are zoned for IVR with a device with domain IDs not within the 97 to 127 range. A loss of connectivity between the hosts and storage devices that are zoned for IVR and the devices in a normal zone might occur.

  Workaround: None. This issue has been resolved.

- CSCsd45429

  Symptom: When performing a switchover, upgrade, or downgrade, logs may be incorrectly synced between supervisor modules. As a consequence, the syslog process is left with some inconsistencies that may cause one or more of the following symptoms:

  - A process may fail while displaying logs for a **show logging** command. After three failures of the syslog process, the switch forces a switchover.
  - Certain small sections of the log may appear out of order, either preceded by or followed by broken log lines, or both. For example, a few lines referring to 2006 Jan 17 may appear embedded between other log lines that refer to 2006 Jan 20, with a broken line before and after the entry.
  - Null characters (ASCII code 0) may appear in the log. These characters cause empty lines to be displayed when using the **show logging** command and appreciably slow down the log output over slow console connections.

  Workaround: None. This issue has been resolved.

- CSCsd78967

  Symptom: If you remove a port from a port channel or shutdown a member port of a port-channel, the ConnUnitPortStatus/State trap is not sent.

  Workaround: None.

- CSCse89151

  Symptom: If you have more than 800 zones in an active zoneset for a single VSAN, your MDS 9000 switch might reload if you move from basic zoning to enhanced zoning and then read the active zoneset information.

  Workaround: None. This issue has been resolved.

- CSCef56229

  Symptom: If an iSCSI initiator is configured differently on multiple switches, iSNS might report more targets to the initiator than the initiator can access. An iSCSI initiator would get a target error if it attempts to establish a connection.

  Workaround: None. This issue has been resolved.

- CSCeg27584

  Symptom: Creating a role that has the VSAN policy “deny” requires an Enterprise License on the switch. If such a role is created on a switch that does not have the license, the switch exhibits different behavior when distribution is turned on as opposed to when distribution is turned off, as follows:

  - If distribution is turned off, creation of the role is rejected.
  - If distribution is turned on, creation of the role succeeds but the VSAN policy continues to be “permit.”

Workaround: None. This issue has been resolved.

- CSCeh33548

  Symptom: Tape devices can only be accessed over an FCIP tunnel in a PortChannel with write acceleration enabled if SID/DID-based load balancing is used in the VSANs.

  Workaround: None. This issue has been resolved.

- CSCeh41099

  Symptom: Protocol and port numbers specified in an IP-ACL assigned to an IPsec profile (crypto map) are ignored. During interoperation between a Microsoft iSCSI initiator with IPsec encryption and Cisco MDS 9000 Family switches, if IPsec is configured in the Microsoft iSCSI initiator (also the IPsec/IKE initiator), the host IPsec implementation sends the following IPsec policy:

  ```
  source IP - Host IP, dest IP - MDS IP
  source port - any, dest port - 3260 (iSCSI), protocol - 6 (TCP)
  ```

  Upon receiving this policy, the protocol and port numbers are ignored and only the IP addresses for the IPsec policy are used. Thus, although iSCSI traffic is encrypted, non-iSCSI traffic (such as ICMP ping) sent by the Microsoft host in clear text is dropped in the MDS switch port.

  Workaround: None. This issue has been resolved.

- CSCeh75500

  Symptom: A device using SANTap may request SANTap to create a session for an ITL that was previously requested, but ITL checking is not robust.

  Workaround: None. This issue has been resolved.

- CSCeh88814

  Symptom: When SANTap is unprovisioned, the control virtual target (CVT) object is not cleaned up on the supervisor module.

  Workaround: None. This issue has been resolved.

- CSCei32317

  Symptom: When configuring a remote SPAN (RSPAN), the Fibre Channel tunnel does not come up if it goes through more than one hop.

  Workaround: None. This issue has been resolved.

- CSCei57342

  Symptom: If a link is isolated because of a fabric-binding database mismatch, a reactivation of the corrected fabric-binding database may not initialize the ports.

  Workaround: Use the **shut** command followed by the **no shut** command to manually disable and then enable the link.

- CSCei58652

  Symptom: When a reconfigure fabric (RCF) frame occurs on a VSAN, the ports may be left in a state where the fabric binding is incorrect.

  Workaround: None. This issue has been resolved.

- CSCei71686

  Symptom: If iSCSI is enabled before FCIP, then the **qos** command that is configurable under a FCIP interface is not available as an option. The reverse is true as well. If FCIP is enabled first, then the **qos** command is not an option for iSCSI interfaces.

  Workaround: None. This issue has been resolved.

- CSCei86399

  Symptom: A TACACS+ key that includes the less than (<) and greater than (>) characters fails when copied to an FTP server, and then copied back to the MDS switch.

  Workaround: None. This issue has been resolved.

- CSCei91968

  Symptom: In a fabric with more than one switch (and under the following circumstances) there is a possibility of CFS or syslogd failing because of a PSS-FULL condition. This issue is caused by leakage in the PSS records stored by the CFS module.

  CFS internal distributions cause a PSS leakage under these conditions:

  - Application registration or de-registration.

    The rate is 1 PSS record or 60 bytes per event.

  - ISL link flap.

    The rate is 2 PSS records per CFS registered application.

    For 10 CFS registered applications, 1000 flaps would cause a leak of about 1M.

  Application distributions in a stable fabric do not result in any PSS leakage. Regular CFS distributions (CFS internal) in a stable fabric do not result in PSS leakage.

  Workaround: None. This issue has been resolved.

- CSCej08751

  Symptom: A Linux host with an iSCSI driver can see only the first eight Logical Units (LUs) of a configured iSCSI virtual target with more than eight LUN maps configured.

  Workaround: None. This issue has been resolved.

- CSCin95686

  Symptom: The RRD graph in the Performance Manager does not refresh on a web client opened in Mozilla or Netscape.

  Workaround: None. This issue has been resolved.

- CSCsb89732

  Symptom: After an upgrade from SAN-OS Release 1.3(2a) to any release earlier than SAN-OS Release 3.0(1), you may see errors such as the following in the syslog file:

```
2005 Sep 15 17:36:55 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:36:56 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:36:59 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:37:43 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:37:44 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:37:47 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:38:31 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:38:32 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:38:35 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
```

  Workaround: None. This issue has been resolved.

- CSCsc09732

  Symptom: If there is a port software failure at the same time as a configuration change for an FCIP interface, the configuration change can fail and subsequent configuration and **show** commands will fail for that FCIP interface.

  Workaround: None. This issue has been resolved.

- CSCsc28722

  Symptom: If you upgrade from a SAN-OS Release 1.3(x) image to a 2.0(x) or 2.1(x) image, ongoing traffic may be disrupted because spurious Registered State Change Notifications (RSCNs) are generated during the upgrade. Hosts that are registered to receive RSCNs using State Change Registration (SCR) get these spurious RSCNs and are disrupted. If you upgrade from a Release 2.0(x) image to a 2.1(x) image, there is no traffic disruption.

  Workaround: None. This issue has been resolved.

- CSCsc31424

  Symptom: Following a switchover, the **no shutdown** command on a port might produce the following error:

  ```
  fc1/1: (error) port channel config in progress - config not allowed
  ```

  Workaround: None. This issue has been resolved.

- CSCsc33788

  Symptom: In rare circumstances, after you issue the **install all** command to upgrade an MDS switch, the upgrade may fail because the installer process fails. When this failure occurs, you may see a message like the following:

  ```
  %CALLHOME-2-EVENT: SW_CRASH alert for service: installer
  The installer failed to respond for 10 times. Exiting ...
  Unable to send exit to installer. Return code -1
  ```

  If you upgrade from 1.3(x) to 2.1 or from 2.0(x) to 2.1 and the upgrade fails, and if after the upgrade failure the supervisor modules are running the new software version, but some modules are running the older software version, then the next attempt to execute the **install all** command will trigger this problem.

  You should not encounter this problem if you upgrade from 2.1 to a higher version.

  Workaround: None. This issue has been resolved.

- CSCsc40012

  Symptom: If you use Telnet or SSH to access an MDS switch, TACACS+ authentication with the domain or user name format does not work.

  Workaround: None. This issue has been resolved.

- CSCsc48919

  Symptom: When a data path on a Storage Service Module (SSM) is congested, diagnostic frames that are delivered as best effort may be dropped. The Online Health Management System (OHMS) may bring down a Fibre Channel port on an SSM when congestion occurs and declare the port as failed.

  Workaround: None. This issue has been resolved.

- CSCsc60283

  Symptom: In rare circumstances, an MDS 9000 Family switch may start displaying the following error messages in the log, several times per second:

  ```
  %KERN-1-SYSTEM_MSG: eepro100: wait_for_cmd_done timeout 0x801249d2 0xf0!
  ```

When this situation occurs, Telnet access through the mgmt0 interface is impossible.

Workaround: None. This issue has been resolved.

- CSCsc72994

  Symptom: If a user does not have a Fabric Manager Server license, a demo or trial license counter for enhanced Fabric Manager Server features starts even when they are not configured. You might see the following message:

  ```
  %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature FM_SERVER_PKG.
  Application(s) shutdown in 119 days.
  ```

  This issue might occur after upgrading to Cisco SAN-OS 2.1(2x). FMS status becomes In Use although none of its features were or are actually used. This situation starts the 120-day evaluation period counter for Fabric Manager Server enhanced features.

  Note This issue does not have any impact on using the Fabric Manager or Device Manager for managing the switch for basic feature operations.

  Workaround: None. This issue has been resolved.

- CSCsc93936

  Symptom: When you attempt to copy a running configuration or startup configuration to a tftp server in a single step, the operation fails.

  Workaround: None. This issue has been resolved.

- CSCsc97070

  Symptom: In Cisco SAN-OS Release 2.1, if more than 250 iSCSI sessions are present on an IPS services module port with proxy initiator mode configured, a port software failure may occur.

  Workaround: None. This issue has been resolved.

- CSCsd02008

  Symptom: During certain timing conditions, such as when a disk takes a long time to register FC4-type and FC4-feature information, IVR may not propagate the FC4-type and FC4-feature information to other VSANs and the information is missing from the name server.

  Workaround: None. This issue has been resolved.

- CSCsd07246

  Symptom: Following a successful login by a host, the **show interface** command lists an interface as “isolated due to port loopback.” In Fabric Manager, the Device Manager shows the same information about the interface.

  Workaround: None. This issue has been resolved.

- CSCsd12831

  Symptom: You might be unable to add or delete a specific user name through the command-line interface, although you can add or delete other user names with no problem. The user name in question does not display in the output of a **show user-account** command; even so, it cannot be added or deleted.

In this situation, you might see the following error message:

```
username <username>  password 0 <passwd>
Internal CLI error: Success error in messaging
Authentication token manipulation error
could not change password for user:<username>
no username <username>
user not present
{could not delete user <username>}
```

Workaround: None. This issue has been resolved.

- CSCsd22920

  Symptom: If the SNMP server location is configured with an empty value, then a subsequent **show running-config** command will only show one character for the SNMP server contact. If the SNMP server location is changed, then the **show running-config** command will show the number of characters in the SNMP server location plus one for the SNMP server contact.

  Workaround: None. This issue has been resolved.

- CSCsd25790

  Symptom: If an internal reconfiguration occurs on an MDS switch, the message that is sent to the log is the same message that is sent when external reconfigure fabric (RCF) frames are sent from the principal switch.

  Workaround: None. This issue has been resolved.

- CSCsd30165

  Symptom: On an MDS 9500 Series switch running Cisco SAN-OS Release 2.1(1b), the output of the **show version** command shows the wrong value for the last reset. This issue does not cause any operational problems on the switch. The output may look like the following:

```
kernel uptime is 137 days 3 hours 49 minute(s) 32 second(s)
 Last reset at -447213060 usecs after Sun Mar 18 05:59:15 2018
   Reason: Not defined
   System version:    Service: §"H
```

  Workaround: None. This issue has been resolved.

- CSCsd53429

  Symptom: After you enter the **ivr zone name** command to configure a zone, the switch displays a message that may be misleading:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name abc
fabric is locked for configuration. Please commit after configuration is done.
switch(config-ivr-zone)#
```

  The message has been changed:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name abc
fabric is now locked for configuration. Please 'commit' configuration when done.
switch(config-ivr-zone)#
```

  Workaround: None. This issue has been resolved.

- CSCsd58774

  Symptom: The following configuration causes excessive data collisions and reduced throughput on the management port of an MDS switch Supervisor 1 module:

  Management port configuration—Speed:100 Mbps, Duplex: Full
  Switch port configuration—Speed: 100 Mbps, Duplex: Full

  Resulting mode on management port—Speed: 100 Mbps, Duplex: Half
  Resulting mode on switch port—Speed: 100 Mbps, Duplex: Full

  Workaround: None. This issue has been resolved.

- CSCsd60578

  Symptom: The problem in FC Write Acceleration on the Storage Services module exhibited itself as a 10% to 15% performance drop once SCSI-Flows are established in both directions in relation to a {SCSI-Initiator, SCSI-Target} pair.

  A bidirectional flow configuration may impact performance in a configuration where SCSI Flow is established for a given SCSI initiator SCSI target pair. For a SCSI flow in one direction, a given node in a SCSI initiator SCSI target pair acts as a SCSI initiator, and for the SCSI flow in the other direction, the same node as a SCSI target.

  This problem applied only to Fibre Channel Write Acceleration on the Storage Services Module (SSM), and has been resolved in SAN-OS Release 3.0(1).

  Workaround: None. This issue has been resolved.

- CSCsd70927

  Symptom: In Fabric Manager, the Performance Manager stops collecting reports after 48 hours. The data from the 48 hours is saved, but the connection to the database appears to be lost.

  Workaround: None. This issue has been resolved.

- CSCsd72822

  Symptom: If a switch has multiple SSMs with the SCSI flow feature enabled, an SSM may fail to come up when you perform an upgrade or reload.

  Workaround: None. This issue has been resolved.

- CSCsd73494

  Symptom: If an iSCSI port receives protocol data units (PDUs) for a write command after it has been aborted by a task management function (TMF), the buffers for these PDUs may be freed twice and this can lead to a port software failure on the iSCSI port.

  Workaround: None. This issue has been resolved.

- CSCsd75284

  Symptom: When multiple tape drives are exposed to a switch over one target port, they appear as multiple LUNs behind the single target port. In this type of configuration, the FCIP link may occasionally get out of sync during error recovery, which may cause the FCIP link to flap.

  Workaround: None. This issue has been resolved.

- CSCsd76429

  Symptom: FCIP tape acceleration causes a flap in the FCIP link when it receives duplicate CHECK CONDITION status frames from a tape device.

  Workaround: None. This issue has been resolved.

- CSCsd81725

  Symptom: If many iSCSI initiators issue writes with immediate or unsolicited data to the iSCSI interface, the result may be a buffer congestion condition that may in turn lead to a B2B credit issue on the FC ports. This may cause these ports to flap.

  Workaround: None. This issue has been resolved.

- CSCsd82449

  Symptom: Mode 1 FCIP compression performance degrades if the Fibre Channel frames received are 1 KB in size.

  Workaround: None. This issue has been resolved.

- CSCsd83775

  Symptom: A Fibre Channel Inter-Switch Link (ISL) does not come up and it displays a fabric binding database mismatch error when fabric binding is activated. Thi s problem may be seen when a supervisor switchover occurs or is performed and this ISL comes up. The fabric binding merge activity detects an incompatible database and fails to bring up the link because an incorrect domain ID is being used by the fabric binding module. The fabric binding module on the switch where the switchover occurs would have cleared its local domain ID and be using a domain ID of zero.

  Workaround: None. This issue is resolved.

- CSCsd92429

  Symptom: The output from the **show tech-support details** command contains the following error message:

  ```
  `show system internal xbar internal all`
  *** cmd parse error ***
  ```

  Workaround: None. This issue has been resolved.

- CSCsd93011

  Symptom: When upgrading to Cisco SAN-OS Release 3.0(1) from an earlier version, the upgrade might fail if there is not enough empty space in the bootflash of the standby supervisor module. The module must be able to hold the kickstart image, the system image, and the SSI image, even though the SSI image does not need to be copied to the standby supervisor module. The upgrade process uses the size of the SSI image to calculate the space required to sync the software images onto the standby supervisor module. The SSI image might be counted as many times as there are Storage Services Modules (SSMs) in the system.

  The SSI image is counted for an SSM if any of the following conditions are met:

  - If the SSI image has been configured in bootvar for the SSM.
  - If the SSI bootvar is specified on the command line when the **install all** command is issued.
  - If the SSI bootvar is manually preset, rather than specified on the command line.

  Workaround: None. This issue has been resolved.

- CSCsf21970

  Symptom: If you issue immediate, back-to-back commands to delete and then create FCIP interfaces, the internal port service might crash.

  Workaround: None. This issue has been resolved.

- CSCsd70102

  Symptom: The Fabric Manager Server may attempt to check out the license after updating it and checking it in. If a user goes into Device Manager and checks in the grace-period license for Fabric Manager Server, the license reactivates and attempts to enable the grace-period license. This results in messages continuously writing to the log that the feature is enabled, even though it is disabled.

  Workaround: None. This issue has been resolved.

Open Caveats

- CSCec28084

  Symptom: The mgmt0 interface responds to ARP requests for the IPS interfaces.

  Workaround: Configure the mgmt0 interface in a separate VLAN from the IPS interfaces.

- CSCsc45880

  Symptom: When suspending or deleting VSANs with no delay between those actions, some Fibre Channel interfaces and member ports in a PortChannel becoming suspended or error-disabled.

  Workaround: Make sure that you suspend and unsuspend one VSAN at a time, and that you wait a minimum of 60 seconds after you issue the **vsan suspend** command before you issue any other configuration command.

- CSCsd19272

  Symptom: The Cisco MDS 9216i switch and MPS-14/2 module do not support an MTU size greater than 8000 bytes. An attempt to set the MTU size greater than 8000 bytes will result in an error.

  Workaround: Reset the value of the MTU size (576 to 8000 bytes) and issue the **no shutdown** command on the interface for normal operation.

- CSCsd47064

  Symptom: The Forwarding Information Base (FIB) process may fail if an IVR zone set push from the Fabric Manager fails because of an SNMP timeout and various switches send conflicting active IVR zone sets.

  Workaround: There are two ways to address the problem:

  - Examine the output of the **show interface mgmt 0** command to see if there is a duplex mismatch that may cause an SNMP timeout.
  - Use the **ivr distribute** command to enable Cisco Fabric Services (CFS) distribution for IVR zone or zone sets and the topology through Inter-Switch Links (ISLs).

- CSCsd94229

  Symptom: On rare occasions, when an active supervisor module is removed from a dual supervisor system, a switchover occurs. After being reinserted, the old active supervisor comes up as the standby supervisor, and the new active supervisor can indicate a kernel panic message.

  Workaround: None.

- CSCsd95862

  Symptom: Cisco MDS 9100 Series switches and the 9216i switch do not handle counter roll-over appropriately and might reset after being up for 497 days. MPS-14/2 modules are also susceptible and could be reset by the supervisor.

  Workaround: None.

- CSCsd97090

  Symptom: The iSCSI I/O failed on a Windows host at 1% packet loss in an IP network.

  Workaround: None.

- CSCsd97376

  Symptom: On the Cisco MDS 9000 4-port 10-Gbps Fibre Channel module, one of the applications would crash during port flaps because of a memory corruption in the application.

  Workaround: None.

- CSCse65400

  Symptom: If a module reloads or reinitializes on its own because of an error, and the port channel has one of its member ports on this module, in rare cases, the peer port of this member port will not forward traffic after the module comes back up.

  Workaround: Issue the **shutdown/no shutdown** command sequence on the port channel. If the problem still persists, issue the **shutdown/no shutdown** command sequence on the affected ports.

- CSCsf98427

  Symptom: If you have SANTap enabled on your SSM, it might reload on its own if your host applications issue FCP requests with an FCP_DL setting of greater than 58K bytes.

  Workaround: None

- CSCsg01963

  Symptom: Multiple RSA implementations might fail to properly handle signatures allowing an attacker to forge RSA signatures.

  Workaround: None.

- CSCsg35972

  Symptom: Under rare conditions, it is possible that a Cisco MDS9216i Switch or an MPS-14/2 module running FCIP might experience port software failures, causing a flap on the Gigabit Ethernet interface. You may see messages like the following:

  ```
  2006 Sep 7 23:13:20 mdspd1 %ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface
  GigabitEthernet1/1 is down (Port software failure)
  2006 Sep 7 23:13:20 mdspd1 %KERN-3-SYSTEM_MSG: Sibyte: Error: CoreId 1 out of range
  2006 Sep 7 23:13:20 mdspd1 %PORT-5-IF_DOWN_INITIALIZING: %$VSAN 2%$ Interface fcip1
  is down (Initializing)
  2006 Sep 7 23:13:20 mdspd1 %PORT-5-IF_DOWN_SOFTWARE_FAILURE: %$VSAN 4094%$ Interface
  iscsi1/1 is down (Port software failure)
  2006 Sep 7 23:13:26 mdspd1 %IPS_SB_MGR-SLOT1-2-PORT_SOFTWARE_FAILURE: Port software
  failure, module 1 port 1
  2006 Sep 7 23:13:26 mdspd1 %IPS_SB_MGR-SLOT1-2-PORT_SOFTWARE_FAILURE: Port software
  failure, module 1 port 1
  2006 Sep 7 23:13:37 mdspd1 %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 4094%$ Interface
  iscsi1/1 is down (Administratively down)
  2006 Sep 7 23:13:46 mdspd1 %ETHPORT-5-IF_UP: Interface GigabitEthernet1/1 is up
  2006 Sep 7 23:13:49 mdspd1 %PORT-5-IF_UP: %$VSAN 2%$ Interface fcip1 is up in mode TE
  2006 Sep 7 23:13:49 mdspd1 %PORT-5-IF_UP: %$VSAN 2%$ Interface fcip1 is up in mode TE
  ```

  Workaround: To reduce the messages or stop them, remove write acceleration if you have it configured for the FCIP interface.

- CSCsh27840

  Symptom: While using an FCIP link for remote SPAN, it is possible that the FCIP link may flap.

  Workaround: Do not use FCIP links for Remote SPAN.

- CSCin95789

  Symptom: When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.

  Workaround: Check the logs to clarify that the correct interface has been selected.

- CSCsc20106

  Symptom: On a Cisco MDS 9020 Fabric Switch, Fabric Manager displays a 4-Gbps Inter-Switch Link (ISL) as a 3-Gbps ISL.

  Workaround: None.

- CSCsc95657

  Symptom: When an administrator configures a serverless backup with QiNetix 5.9, the first time (or each time the disks are reconfigured using Volume Explorer on CommVault) the backup fails with a Reservation Conflict error on the disk.

  Workaround: Reset the disk and retry the configured serverless backup.

- CSCsd15794

  Symptom: If the iSNS client has registered with the iSNS server, and does not send any protocol messages to server, the the iSNS server might not timeout idle sessions from the iSNS client.

  Workaround: Clear the session explicitly from the iSNS Client side.

- CSCsd21187

  Symptom: If an iSNS client tries to register a portal separately after registering the network entity and storage node object with the Cisco MDS iSNS server, the portal registration might fail.

  Workaround: Register the portal at the same time as the network entity and storage node object registration

- CSCsd34882

  Symptom: The SAN-OS software creates a syslog message after a configuration change through the command-line interface The syslog message looks like this:

  ```
  switch# 2006 Feb 8 09:00:33 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
  from pts/1 (dhcp-peg3-vl30-144-254-7-182.cisco.com)
  ```

  Using the Fabric Manager to make the same configuration change does not result in the same syslog message:

  ```
  switch# 2006 Feb 8 09:00:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface
  fc1/5 is down (Administratively down)
  ```

  Workaround: None.

- CSCsd51194

  Symptom: When a switchover occurs on a switch that is the master for Virtual Router Redundancy Protocol (VRRP) interfaces, the switchover may cause a minor delay. As a result, the VRRP backup (occurring elsewhere) may assume the role of the VRRP master.

  Workaround: Increase the VRRP advertisement interval for these interfaces.

- CSCsd52037

  Symptom: A serverless backup of a volume spanning multiple tapes does not work with CommVault QiNetix 5.9 because CommVault QiNetix 5.9 is not able to determine the end of Tape.

  Workaround: None.

- CSCsd79575

  Symptom: In interop mode 4, a zone merge can cause a default zone policy change. This change can occur if one of the switches involved in the merge has no active zone set and a default zone policy permit, which can lead to potential traffic disruption.

  In McDATA versions lower than 8.x, if one of the switches involved in a zone merge has no active zone set and the default zone policy is permit, the switch accepts the active zone set of the neighbor switch and changes its default zone policy to that of the neighbor switch. However, for version 8.x and higher, a difference in the default zone policy between two switches results in the link being isolated during a zone merge.

  The MDS family of switches behaves in accordance with McDATA versions lower than 8.x. Therefore, traffic may be disrupted because a link can become isolated if a merge occurs between an MDS switch and a McDATA switch running version 8.x or higher.

  Workaround: Before you bring up a link, make sure that the default zone policies are the same on both switches.

- CSCsd79938

  Symptom: After using the **ip access-group** command to configure an access list for the mgmt0 interface and saving the running configuration to the startup configuration, the **ip access-group** command is not present following a reboot of the running configuration. However, the command is in the startup configuration, and the access list is still in the configuration, but the access list is not applied to the mgmt0 interface.

  Workaround: Reconfigure the **ip access-group** command or issue a **copy startup-config running-config** command to replace the **ip access-group** command.

- CSCsd81137

  Symptom: Duplicate entries within an FC alias might cause an ISL isolation between your MDS 9000 switch and a Brocade switch.

  Workaround: Remove duplicate entries from the Brocade switch and the link will come up.

- CSCsd87853

  Symptom: When the default gateway is configured for multiple CPP interfaces, the running configuration retains the default gateway associated with only one of the CPP interfaces.

  Workaround: Re-configure the default gateways of the CPP interfaces upon a reboot or a switchover.

- CSCsd89872

  Symptom: When using Cisco MDS SAN-OS Release 2.1(2e) or earlier to configure PortChannels, the following message may be displayed:

  ```
  Last membership update failed: port-channel: required service is not responding
  (err_id 0x402B No port
  ```

  If this issue occurs, any attempt to delete the PortChannel will fail and no additional operations can be performed on that specific PortChannel that gave the error.

Workaround: Upgrade from Cisco SAN-OS Release 2.1(2e) or earlier to Release 3.0(2a) to prevent the problem from occurring. If the problem has already occurred, an upgrade to Release 3.0(2a) will not correct the problem. Issue the **write erase** command and reboot the system to correct this problem.

- CSCsd94019

  Symptom: In Fabric Manager, the Device Alias sort function does not work correctly.

  Workaround: None.

- CSCsd94718

  Symptom: In Fabric Manager, the local zone database is not synchronized.

  Workaround: None.

- CSCsd99599

  Symptom: In interop mode 3, when a regular or IVR zone set is activated from an MDS switch and the active zone set contains aliases, the aliases in the corresponding zone set in the full configuration database will be removed.

  Workaround: To maintain the alias information, activate a zone set containing aliases from a Brocade switch.

- CSCse12209

  Symptom: When using Fabric Manager and SNMP, a login does not occur when a user ID contains a backslash "\".

  Workaround: None.

- CSCse13769

  Symptom: Unplugging the 10-Gbps X2/SC optics from the 10-Gbps module may cause the transmission of buffer-to-buffer credits (BB_Credits) to become incorrectly programmed. This situation may impact the performance of load balanced traffic on the 10-Gbps Fibre Channel port.

  Workaround: Always perform a graceful shutdown of the port using the **shutdown** command prior to removing the 10-Gbps X2/SC optics.

- CSCse14032

  Symptom: The ISNS server process terminates when ISNS-SERVER is enabled on a switch that has more than 100 iSCSI initiators.

  Workaround: None.

- CSCse22145

  Symptom: CFS coordinated distribution events are not logged in the syslogs.

  Workaround: Use the **show cfs internal session-history name** command to see the coordinated distribution events that are logged.

- CSCse36768

  Symptom: The Cisco MDS 9100 and 9200 Series switches might see excessive debugging messages sent to the CompactFlash causing a rare condition where the CompactFlash could lock up. If this occurs, you might experience an inability to save a new configuration to the Flash and a reboot of the switch is required to recover from this failure. If a successful administrative function requires a write to CompactFlash or there is an update within the fabric, then unexpected behavior might occur.

  Workaround: None.

- CSCse41442

  Symptom: Issuing the **show zone member fcid** command on your Cisco MDS 9000 switch might not display the zones with that member FC ID.

  Workaround: Configure zone membership by using either pWWN, pWWN + LUN, FC ID, or FC ID + LUN.

- CSCse70275

  Symptom: The Qlogic 2460 HBA fails to remote boot when it connects to a VT instantiated by SANTap on the SSM because the Qlogic 2460 BIOS sends a test ready unit with an invalid command reference number (CRN) and task attribute field. This same HBA can boot when SANTap and the SSM are not part of the configuration.

  Workaround: Use the Qlogic 2340 HBA.

- CSCse71420

  Symptom: If you have multiple switches with IVR, and there is a mismatch of IVR VSAN topology and IVR zones which were corrected later, you might get an error message in the logs %FSPF-3-IPC_PROC_ERR: Error in processing IPC message : Opcode = 68, Error code = 401a0013

  Workaround: None.

- CSCse84811

  Symptom: In a system with autocreate PortChannel configured, if there are multiple link flaps or configuration changes on a PortChannel, the PortChannel Manager process memory might run out causing the PortChannel Manager process to crash.

  Workaround: Issue the **write erase** command and reload the switch.

- CSCse88606

  Symptom: Setting a value higher than 4 for the maximum number of times a packet is retransmitted before TCP closes the connection might product unexpected results. This would occur during a link FCIP tunnel recovery after a short downtime.

  Workaround: Configure the TCP maximum retransmissions to values between 1 and 4 only.

- CSCse99087

  Symptom: A user called snmp-user can successfully log into an MDS switch through the CLI, but cannot log in through Fabric Manager or Device Manager. The login attempt fails with this error:
  `SNMP: Unknown username`

  Workaround: None.

- CSCsf18552

  Symptom: When activating an IVR zone set or changing an IVR configuration, the IVR process might crash. The IVR process restarts and status is restored to a pre-crash state. Neither existing traffic nor the configuration is affected.

  Workaround: None. When the IVR process restarts after the crash, the inconsistent database gets corrected.

- CSCsf96043

  Symptom: No alerts are issued for FCS errors on the sup-fc0 port even though it might affect Fibre Channel communication.

  Workaround: None.

- CSCsg03171

  Symptom: The dynamic port VSAN membership (DPVM) failed after the number of F ports exceeded 64 and a port flap occurred.

  Workaround: Keep the number of F ports in a switch below 64.

- CSCsg12020

  Symptom: If your switch is up for a long period of time, such as more than 100 days, zone set activation in Fabric Manager might not reflect the latest results and active-local differences may still be shown.

  Workaround: Close and reopen Fabric Manager with the "Accelerate Discovery" option unchecked. This reflects the latest change, but might need to be done after every change.

- CSCsg15392

  Symptom: If a Generation 1 module has any port that is administratively up, but operationally down when you upgrade from SAN-OS Release 2.x to either Release 3.0(1) or Release 3.0(2x), you might experience traffic disruption on that module.

  Workaround: Use the **shutdown** command to shut all the ports operationally down and administratively up on all the Generation 1 modules before upgrading from SAN-OS Release 2.x to Release SAN-OS 3.0(x) or Release 3.0(2x). After the upgrade is complete, the ports can be brought to an administratively up state using the **no shutdown** command.

- CSCsg29400

  Symptom: If you use Device Manager to create a target initiator and then you select **Edit**, Device Manager allows the entry to be a host address with a /24 mask, but it should only allow a /32 mask for a host address.

  Workaround: Use Device Manager to remove the entry.

- CSCsg62359

  Symptom: If a user attempts to log in using TACACS+ authentication to an MDS switch or an SSH server configured on the switch, the login might fail if password-authentication is the first login method the user tries.

  Workaround: Use the keyboard-interactive method as the first login method for SSH.

- CSCsg82792

  Symptom: When trying to copy a core file from an MDS switch to a location such as a TFTP server, the system asks for the core filename, but the actual filename is not visible in the CLI.

  Workaround: To show the supervisor module on which a process crashed and show the process ID, enter the **show cores** command. To transfer the core file, enter the full command:
  copy core://*supervisor mod number/pid* **tftp:**

- CSCsh24256

  Symptom: It is possible for the hardware interface used to access SFPs and temperature sensors on modules to lock up. This inhibits the detection of a subsequent removal or insertion of an SFP and results in the failure to read a module's temperature sensors.

  Workaround: Reload the module to recover the sensor.

- CSCsh83200

  Symptom: If you remove a fan tray module from an MDS 9500 series switch that is running Cisco MDS SAN-OS Release 3.0(1), 3.0(2), 3.0(2a) 3.0(2b), 3.0(3), 3.1(1), 3.1(2) or 3.1(2a), the switch shuts down if you do not replace the fan tray module within 170 seconds. (In all other SAN-OS releases, you have 250 seconds to replace it.)

Workaround: None.

- CSCso63465

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

  Workaround: Do not use LUN 0x45F0 and LUN 0x50F0 when Generation 2 modules are present in the fabric.

- CSCsd85503

  Symptom: If you use the PortChannel Wizard to configure a PortChannel, Fabric Manager may display a message that includes “portChannelRowStatus: inconsistentValue” when you click Finish in Step 3. If you see this message, it is possible that the wizard is using an existing PortChannel ID to make a new PortChannel.

  Workaround: Change the PortChannel ID for both switches and click **Finish** again.

- CSCsd92433

  Symptom: Additional information is needed from the **show tech-support** command.

  Workaround: None.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at:
http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html.
For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:
http://www.ibm.com/storage/support/2062-2300/

Send documentation comments to mdsfeedback-doc@cisco.com.

Release Notes

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

Compatibility Information

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

Regulatory Compliance and Safety Information

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

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

Cisco Fabric Manager

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

Command-Line Interface

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

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

Troubleshooting and Reference

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

Installation and Configuration Note

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

Send documentation comments to mdsfeedback-doc@cisco.com.

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Send documentation comments to mdsfeedback-doc@cisco.com.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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

Send documentation comments to mdsfeedback-doc@cisco.com.