

Send documentation comments to mdsfeedback-doc@cisco.com



Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.0(2a)

Release Date: July 18, 2006

Text Part Number: OL-8795-03 V0

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 34.



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	07/18/2006	Created release notes
B0	07/24/2006	Modified DDTS CSCse33080 . Modified the Upgrading with IVR Enabled section.
C0	08/2/2006	Fixed the status of DDTS CSCsd89872 .
D0	08/7/2006	Clarified DDTS CSCsd89872 description.
E0	08/22/2006	Added DDTS CSCse65400 . Modified the Downgrading from Cisco MDS SAN-OS Release 3.0(2a) .
F0	09/5/2006	Added DDTS CSCse88606 .
G0	09/7/2006	Added DDTS CSCec28084
H0	09/22/2006	Added the external crossbar module part number.



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

© 2008 Cisco Systems, Inc. All rights reserved.

Table 1 Online History Change

Revision	Date	Description
I0	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.
J0	12/13/2006	Added DDTS CSCsd15794 , CSCsd21187 , CSCsd81137 , CSCsd99599 , CSCse22145 , CSCse31881 , CSCse41442 , CSCse44834 , CSCse48977 , CSCse52582 , CSCse62012 , CSCse69783 , CSCse70275 , CSCse71420 , CSCse72182 , CSCse79582 , CSCse85609 , CSCse88880 , CSCse93991 , CSCse98656 , CSCsf12069 , CSCsf18552 , CSCsf18884 , CSCsf19419 , CSCsf21575 , CSCsf96043 , CSCsf97117 , CSCsf98427 , CSCsg01963 , CSCsg10555 , CSCsg12020 , CSCsg13769 , CSCsg15392 , and CSCsg19198 .
K0	02/01/2007	Added DDTS CSCsg03171 .
L0	02/22/2007	Added DDTS CSCsd92433 , CSCsd97376 , CSCse99087 , CSCsf27608 , CSCsf30937 , CSCsg05037 , CSCsg12096 , CSCsg29400 , CSCsg31334 , CSCsg35972 , CSCsg52197 , CSCsg62359 , CSCsg80637 , CSCsg82792 , CSCsg94749 , CSCsg96497 , CSCsg99049 , CSCsh27840 , and CSCsh31236 .
M0	02/27/2007	Added DDTS CSCsg72224 and CSCsh40033 .
N0	04/04/2007	Added DDTS CSCsh66010 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”.
O0	06/11/2007	Added DDTS CSCsg41556 , CSCsh24256 , CSCsi27133 , and CSCsi33540 .
P0	07/18/2007	Added DDTS CSCsj07363 and CSCsj19105 . Removed DDTS CSCei82909 .
Q0	08/24/2007	Added DDTS CSCsg18834 .
R0	09/28/2007	Added DDTS CSCeh35635 , CSCsi49231 , and CSCsj65565 .
S0	10/23/2007	Removed DDTS CSCsh31236 . Added information about Downgrading from Cisco SAN-OS Release 3.2(1) to the “Limitations and Restrictions” section.
T0	04/30/2008	Added DDTS CSCso63465 .
U0	11/13/2008	Added the “Performing a Nondisruptive Software Upgrade on Generation 1 Modules” section.
V0	11/18/2008	Added DDTS CSCso72230 .

Send documentation comments to mdsfeedback-doc@cisco.com

Contents

This document includes the following sections:

- [Introduction, page 3](#)
- [System Requirements, page 3](#)
- [Upgrading Your Cisco MDS SAN-OS Software Image, page 8](#)
- [New Features in Cisco MDS SAN-OS Release 3.0\(2a\), page 14](#)
- [Limitations and Restrictions, page 14](#)
- [Caveats, page 17](#)
- [Related Documentation, page 34](#)
- [Obtaining Documentation, page 36](#)
- [Documentation Feedback, page 37](#)
- [Cisco Product Security Overview, page 37](#)
- [Obtaining Technical Assistance, page 39](#)
- [Obtaining Additional Publications and Information, page 40](#)

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(2a) and includes the following topics:

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- [Components Supported, page 4](#)
- [Determining the Software Version, page 7](#)
- [Downloading Software, page 8](#)

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	M95S2K9-3.0.2a	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.0.2a	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-3.0.2a	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-3.0.2a	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 SSM
M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with SSM	

Send documentation comments to mdsfeedback-doc@cisco.com

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-SF1-K9	MDS 9500 Supervisor/Fabric-I module.	

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.	

Send documentation comments to mdsfeedback-doc@cisco.com

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.



Note

If you would like to request a copy of the source code under the terms of either GPL or LGPL, please send an e-mail to mds-software-disclosure@cisco.com.

Use the following guidelines to nondisruptively upgrade your Cisco MDS SAN-OS Release 3.0(2a):

- 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](#).
- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco SAN-OS Release 3.0(1) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Follow this upgrade path for your current release:
 - Upgrading from Cisco SAN-OS Release 1.x to Release 3.x requires that you upgrade first to Release 1.3(4a), then upgrade to Release 2.1(2b), and then upgrade to Release 3.0(2a) .
 - Upgrading from Cisco SAN-OS Release 2.0(2b), 2.0(2c), 2.0(3), 2.1(2b), 2.1(2c), 2.1(2d), 2.1(2e), or 3.0(1) allows you to nondisruptively upgrade directly to Release 3.0(2a). 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 Release 3.0(2a).
 - Upgrading from other Cisco SAN-OS Release 2.x releases to Release 3.x requires that you upgrade first to Release 2.1(2b), and then upgrade to Release 3.0(2a).
 - If you have IVR enabled and you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a), then there are additional steps you should follow before upgrading. See [“Upgrading with IVR Enabled” section on page 10](#).
 - If you have FICON enabled and you are upgrading from Cisco SAN-OS Release 1.x to Release 3.x then first upgrade to Release 1.3(4a), then upgrade to Release 2.0(2b), and then upgrade to Release 3.0(2a).

Send documentation comments to mdsfeedback-doc@cisco.com

- The traffic on all Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. 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 is disrupted during upgrades or downgrades. Layer 2 switching is not disrupted under the following conditions:
 - Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the [Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images](#).
 - All SSM 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 the “[Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0\(2a\)](#)” section on page 12.
 - 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.



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

For more information on determining software compatibility, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#).

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:

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.

The caveat associated with this issue is CSCsm62295.

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, syslog messages indicate RDI failure and the flapped ISL 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(2a) 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 8.

To upgrade from Cisco SAN-OS Release 2.1(1a), 2.1(1b), or 2.1(2a) to Release 3.0(2a) 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 `fdomain domain id static vsan vsan id` command to configure the static domains.

Send documentation comments to mdsfeedback-doc@cisco.com



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

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



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

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

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
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(2a) in the “[Upgrading Your Cisco MDS SAN-OS Software Image](#)” section on page 8.

If you are adding new switches running Cisco MDS SAN-OS Release 3.0(x), upgrade all your existing switches to Release 3.0(2a) 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
```

Send documentation comments to mdsfeedback-doc@cisco.com

```

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(2a)

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 Release 3.0(2a) to avoid any traffic disruption.

For more information on upgrading SAN-OS software, see the [“Upgrading Your Cisco MDS SAN-OS Software Image” section on page 8](#).

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
    
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
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

Send documentation comments to mdsfeedback-doc@cisco.com

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 in this 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 3.1(2b)), 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(2a)

This section describes the new features introduced in this release. For more information about the features listed, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

**Note**

These release notes are specific to this release. For the complete Release 3.x documentation set, see the [“Related Documentation” section on page 34](#).

There are no new features available for this release.

Limitations and Restrictions

This section lists the limitations and restrictions for this release.

Downgrading from Cisco MDS SAN-OS Release 3.0(2a)

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.0(2a):

Send documentation comments to mdsfeedback-doc@cisco.com

- 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. Use 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 Release 2.1(2b), then downgrade to Release 1.3(4a), and then downgrade to your 1.x release.
 - You can downgrade nondisruptively from Release 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), or 3.0(1). Downgrading to other Cisco SAN-OS Release 2.x releases from Release 3.x requires that you downgrade first to 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 Release 2.0(2b), then downgrade to Release 1.3(4a), and then downgrade to your 1.x release.
- Traffic on all Gigabit Ethernet ports is disrupted on an 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 an MPS-14/2 module is online in the switch. Otherwise, the downgrade will disrupt traffic.
- Layer 3 switching on SSM ports is disrupted on upgrades or downgrades.
- Layer 2 switching on SSM ports is not disrupted under the following conditions:
 - All SSM 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** configuration mode 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 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 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:

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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

iSNS

The iSNS client and server are not supported in 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(2a), see the [“Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0\(2a\)”](#) section on page 12.

CWDM SFPs

Some 2-Gbps CWDM SFPs do not 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.

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 exists 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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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*

DDTS Number	Software Release (Open or Resolved)	
	3.0(2)	3.0(2a)
Severity 2		
CSCec28084	O	O
CSCsc45880	O	O
CSCsd47064	O	O
CSCsd95862	O	R
CSCsd97376	O	O
CSCse14087	O	R
CSCse33080	O	R
CSCse35720	–	O
CSCse44834	O	O
CSCse56522	O	R
CSCse57269	O	O
CSCse65400	O	O
CSCse67109	O	O
CSCse72182	O	O
CSCse85609	O	O
CSCsf18884	O	O
CSCsf21575	O	O
CSCsf98427	O	O
CSCsg01963	O	O
CSCsg35972	O	O
CSCsg72224	–	O
CSCsh27840	O	O
CSCsi33540	–	O
CSCsi49231	O	O
CSCsj19105	–	O
CSCsj65565	–	O
CSCso72230	–	O
Severity 3		
CSCeg55238	O	R
CSCin95789	O	O

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 4 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	3.0(2)	3.0(2a)
CSCsc95657	O	O
CSCsd15794	O	O
CSCsd19272	O	O
CSCsd21187	O	O
CSCsd34882	O	R
CSCsd51194	O	O
CSCsd52037	O	O
CSCsd79938	O	O
CSCsd81137	O	O
CSCsd89872	O	O
CSCsd99599	O	O
CSCse12209	O	O
CSCse13769	O	R
CSCse13999	O	R
CSCse14032	O	R
CSCse22145	O	O
CSCse31881	O	O
CSCse36768	O	R
CSCse41442	O	O
CSCse42040	O	O
CSCse48977	O	O
CSCse52582	O	O
CSCse62012	O	O
CSCse69783	–	O
CSCse70275	O	O
CSCse71420	O	O
CSCse79582	O	O
CSCse88606	O	O
CSCse88880	O	O
CSCse93991	–	O
CSCse98656	O	O
CSCse99087	O	O
CSCsf12069	O	O
CSCsf18552	O	O
CSCsf19419	O	O

Send documentation comments to mdsfeedback-doc@cisco.com

Table 4 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	3.0(2)	3.0(2a)
CSCsf27608	O	O
CSCsf30937	–	O
CSCsf96043	O	O
CSCsf97117	O	O
CSCsg03171	O	O
CSCsg05037	O	O
CSCsg10555	O	O
CSCsg12020	O	O
CSCsg12096	O	O
CSCsg13769	O	O
CSCsg15392	O	O
CSCsg18834	O	O
CSCsg19198	–	O
CSCsg29400	O	O
CSCsg41556	O	O
CSCsg52197	–	O
CSCsg62359	O	O
CSCsg80637	–	O
CSCsg82792	O	O
CSCsg94749	–	O
CSCsg96497	–	O
CSCsg99049	–	O
CSCsh24256	O	O
CSCsh40033	–	O
CSCsh66010	–	O
CSCsh83200	O	O
CSCsi27133	–	O
CSCsj07363	–	O
CSCso63465	O	O
Severity 4		
CSCsg31334	–	O
Severity 6		
CSCeh35635	–	O
CSCsd92433	O	O

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Resolved Caveats

- 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. This issue has been resolved.
- CSCse14087

Symptom: During a link flap, the FCIP tape acceleration feature could get into a state where if the tape is slow in responding, the backup or restore operation may fail.

Workaround: None. This issue has been resolved.
- CSCse33080

Symptom: In some cases, after a nondisruptive upgrade (or downgrade) of 48-port and 24-port 4-Gbps Fibre Channel switching modules from Cisco SAN-OS Release 3.0(1) to Release 3.0(2) (or a downgrade from Release 3.0(2) to Release 3.0(1)), the next port flap could result in oversubscribed ports coming up in error-disabled state.

Workaround: None. This issue has been resolved.
- CSCse56522

Symptom: In some cases, when a VSAN is in suspended mode, the switch with the suspended VSAN does not appear in the table on the Information pane of the GUI.

Workaround: None. This issue has been resolved.
- CSCeg55238

Symptom: Files created using the **fcalyzer local** command cannot be copied or viewed. Fibre Channel analyzer runs as root, and it creates files with the owner as root. The correct file creation masks are not set when the file is created, so no user other than root can read or copy the file.

Workaround: None. This issue has been resolved.
- CSCsd34882

Symptom: The Cisco 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 generates a different 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. This issue has been resolved.
- CSCse13769

Symptom: In some cases of link flapping (a link down or up due to removal or insertion of cables or transceivers) on 10-Gbps ISLs, an early LR might arrive before the ELP exchange is complete and would trigger a transmit credit update to the port. This causes the switch port transmit credit to program to the default value of one (1) instead of the actual number configured. This might cause an impact to performance.

Workaround: None. This issue has been resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCse13999

Symptom 1: SNMP events are not visible in Fabric Manager because Fabric Manager is unable to register to receive SNMP notifications, even though Device Manager is registered to receive SNMP notifications from the MDS switch.

Symptom 2: Cisco EMC Call Home does not send call home messages. Cisco EMC Call Home is a new feature for Cisco SAN-OS Release 3.0(1). This does not affect the other Cisco Call Home features.

Workaround: None. This issue has been resolved.
- CSCse14032

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

Workaround: None. This issue has been resolved.
- 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. This issue has been resolved.

Open Caveats

- CSCed16845

Symptom: Occasionally, the Common Information Model (CIM) server may be automatically restarted because of an internal error. In this case, the connected CIM client is disconnected.

Workaround: You must explicitly reconnect the CIM client to the CIM server.
- CSCeg12383

Symptom: On rare occasions, the PortChannels with FCIP interface members fail to come up when the switch reboots. This occurrence happens when the startup configuration has a default switch port trunk mode setting that does not match the configured trunk mode for PortChannel members (FCIP interfaces). Also, the startup configuration shows any explicit switch port trunk mode setting for the PortChannel.

Workaround: Reconfigure the switch port trunk mode on the PortChannel.
- CSCeg37598

Symptom: The iSNS server might crash when iSCSI is disabled and iSNS is enabled using Fabric Manager.

Workaround: None.
- CSCse35720

Symptom: If you have a Port Channel with multiple FCIP tunnels, and Write Acceleration is enabled on the the FCIP tunnels, the end device might reboot with an error after the Port Channel comes up or if fcping is issue to that device.

Workaround: Disable FCIP Write Acceleration on all FCIP tunnels in the Port Channel or configure only a single FCIP tunnel in the Port channel.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCse44834
Symptom: Under certain circumstances, processing a response to the recovery message might cause a software failure. If the host receives a status from the host-end FCIP tunnel for a tape read or Write IO and is slow in responding with a status confirmation, the recovery message is sent by the FCIP Tape Acceleration feature to the host.
Workaround: None.
- CSCse57269
Symptom: You cannot bind more than one FCIP interface on Gigabit Ethernet port 2 on an MPS-14/2 module in Cisco SAN-OS Release 3.0(1) and Release 3.0(2).
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.
- CSCse67109
Symptom: On a 24- or 48-port Fibre Channel switching module, if all ports in a port group are switching traffic at the ports group's full bandwidth, and there is a mix of over-ubscribed and full rate ports, the first four ports in the group might exhibit a transmit credit underrun condition.
Workaround: Reset the 24- or 48-port FC switching module, or upgrade to Cisco SAN-OS Release 3.0(2a).
- CSCse72182
Symptom: Certain CIM requests leak memory over time.
Workaround: None.
- CSCse85609
Symptom: This problem is observed in Interop mode 4, if IVR is being used with Mcdata switches. The SW-RCSN generated by McData switches does not contain the port WWN and node WWN as required by the Fibre Channel standard. In Cisco MDS SAN-OS Release 3.0(1) and earlier, IVR expected the port WWN in the SW-RCSN. When a device attached to a McData switch goes down, the IVR process does not understand the SW-RCSN generated by the McData switch. As a result, the IVR process does not propagate this information in other VSANs and the device entry continues to stay in the name server database in other VSANs.
Workaround: Remove the device from the IVR active zone set to get rid of the stale entry.
- CSCsf18884
Symptom: Removing all devices belonging to a source domain from active zone set or an unreachable source domain might cause traffic disruption from other existing source domains.
Workaround: Add a new member belonging to a source domain that is not currently configured to communicate with the destination domain, to the IVR zone set and reactivate the IVR zone set.
- CSCsf21575
Symptom: A CFS merge might fail if all the switches in a large fabric are reloaded.
Workaround: Issue the **ivr commit configuration** command to perform a blank commit and bring up CFS from the failed state.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.

- CSCsg72224

Symptom: The fabric login (FLOGI) process fails while new hosts are initializing. The **show flogi internal event error** command shows that a module is not present.

Workaround: Re-install the module.

- 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.

- CSCsi33540

Symptom: On a 4-Gbps Fibre Channel module, PLOGI accepts were discarded because the port was initially an F port, but had been changed to an E port.

Workaround: To resolve this issue, follow these steps:

1. Remove the E port from the PortChannel.
2. Reconfigure the port as an F port.
3. Issue the **shut** command on the port.

Send documentation comments to mdsfeedback-doc@cisco.com

4. Change the port to an E port
 5. Add the port to the PortChannel.
 6. Enter the **no shut** command on the port.
- CSCsi49231

Symptom: 100% CPU utilization was seen on an MDS switch. It was caused by repeated fabric logins (FLOGIs) on a particular port. This situation can occur if a host cannot log in because the allocation of the FC ID fails, and keeps re-trying using a specific pattern of Source FC IDs (S_IDs) for the FLOGI frame.

Workaround: The interface will now be error-disabled for too many FLOGI failures.

To troubleshoot the configuration and find the reason for the FC ID allocation failure, examine the messages in the syslog. Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for detailed information about FLOGI, FC IDs, and FC ID allocation for HBAs.
 - CSCsj19105

Symptom: A crash might occur in the intelligent line card (ILC) helper process when provisioning or deprovisioning a storage application on the SSM card.

Workaround: If the ILC helper dumps core memory three times, reboot the switch for it to function normally. Use the **show cores** command to determine if the ILC helper has dumped core memory.
 - CSCsj65565

Symptom: Spectra Logic tape drives require a unique area ID.

Workaround: Add the company OUI ID to the switch database so that the switch can assign unique area IDs to the Spectra Logic tape drives.
 - CSCso72230

Symptom: In rare instances, the following Generation 2 modules might reload:

 - 12-port 4-Gbps Fibre Channel module
 - 24-port 4-Gbps Fibre Channel module
 - 48-port 4-Gbps Fibre Channel module
 - 4-port 10-Gbps Fibre Channel module

The output of the **show logging log** command will have events like those shown below. In the following output, module 7 is the supervisor and module 12 is the module that reloaded.

```
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 7 (serial: JAE1134UR88)
reported warnings on ports 7/1-7/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 8 (serial: JAE1134UOTD)
reported warnings on ports 8/1-8/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:35 fcd95c41 %XBAR-5-XBAR_STATUS_REPORT: Module 12 reported status
for component 88 code 0x40240015.
2008 Jul 15 19:39:35 fcd95c41 %MODULE-2-MOD_DIAG_FAIL: Module 12 (serial: JAE1136VU6L)
reported failure on ports 12/1-12/24 (Fibre Channel) due to Fatal runtime Arb error.
(DevErr is bitmap of failed modules) in device 88 (device error 0x800)
"show logging onboard" will show log similar to the one below for the reloaded module:
Logging time: Tue Jul 15 19:39:28 2008
machine check: process swapper (0), jiffies 0x744af3a4
Free pages in zone[0]:0x4a70,zone[1]:0x0,zone[2]:0x0
Stack: c000dd58 c001eefc c000b2c4 c000ae98 d2060e10 c003d7a4 c00f869c c0045cdc
d196c584 d196d100 c000c31c c000c3e4 c000ae90 c000c910 c000c924 c0008948 c01ca610
c0000394
.....
```

Send documentation comments to mdsfeedback-doc@cisco.com

.....

Workaround: None. The chance of a module reload occurring again on the same module is very rare. Therefore, continued use of the module is acceptable.

A software workaround for this issue exists in SAN-OS Release 3.3.(2) and NX-OS Release 4.(1b). Upgrading to one of those releases will help decrease instances of modules reloads.

- 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.

- 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 are 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.

- 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).

- 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.

- CSCsc95657

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

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.
- 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
- 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.
- 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: Reissue 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.
- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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 are 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.
- 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.
- CSCse31881

Symptom: If there are IPFC interfaces configured on an SSM, you might experience issues if you downgrade from SAN-OS Release 3.x to Release 2.x.

Workaround: Before downgrading, remove the IPFC interface on the module and then recreate the IPFC interface after the downgrade is complete.
- 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.
- CSCse42040

Symptom: If you try to create a user with a weak password, it fails. Subsequent attempts to create the same user with a strong password also fail because of an inconsistentValue error. This is because when the creation failed in the first set, the undo is not handled completely.

Workaround: Issue the **no snmp-server username** command in the CLI before the user creation is attempted a second time.
- CSCse48977

Symptom: Fabric Manager Zone Editor may open slowly when a large number of zones are present (for example, 8000 zones).

Workaround: None.
- CSCse52582

Symptom: In Fabric Manager, a device moved from one VSAN to another, might still show up in the Edit IVR Local Full Zone Database dialog box as in the old VSAN. Clicking the refresh button has no effect.

Workaround: Click the rediscover button to rediscover the fabric and then press the refresh button on the Zone dialog box.
- CSCse62012

Symptom: Issuing the **setup** command might fail after a supervisor switchover, even though the standby supervisor is already in HA-standby state.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: None.

- CSCse69783

Symptom: RMON alarms do not appear in the running configuration when they are configured through Threshold Manager using 64-bit alarms.

Workaround: Use the **show rmon hcalarms** command to view the configuration.

- 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.

- CSCse79582

Symptom: In Fabric Manager, the active zone set name might display in bold italics instead of plain italics, indicating a pending zone set when there is no actual change pending.

Workaround: None.

- CSCse88606

Symptom: Setting a value higher than 4 for the maximum number of times a packet is retransmitted before TCP closes the connection might produce 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.

- CSCse88880

Symptom: You might experience a system reboot if you are using custom VSAN role-based access control for SNMP users.

Workaround: None.

- CSCse93991

Symptom: An FC domain restart disrupts the Invista controller connectivity with the SSM.

Workaround: None.

- CSCse98656

Symptom: Your system might not recover after some types of chassis clock failure and your Supervisor modules might reboot continuously. If the active supervisor reboots, it might report the following message before reboot:

```
2006 Aug 2 14:36:35 svb-san-m9513-3 %MODULE-2-MOD_DIAG_FAIL: Module 7
(serial: JAB102100U3) reported failure on ports 7/1-7/1 (Supervisor Inband)
due to Fatal runtime sync error. (DevErr is bitmap of failed modules) in
device 88 (device error 0x40)
```

Workaround: None.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.
- CSCsf12069

Symptom: A lock request for device-alias might fail, even though the lock is not acquired in the fabric for device-alias. This issue does not happen in a single switch setup but can happen when there are two or more switches with device alias enabled for CFS.

Workaround: Follow these steps:

 1. Use the **show system internal mts sup apps** command to find out the sap of the application where the lock request is failing.
 2. Execute the **cfs internal decrement-uncoord sap** command. For device-alias, execute the **cfs internal decrement-uncoord 135** command.
 3. Reissue the configuration command.
- 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.
- CSCsf19419

Symptom: On FICON enabled VSANs, if you perform prohibit or unprohibit operations to change the prohibit matrix on a large number of ports, the Cisco MDS 9513 switch might take more time to respond than the ptov protocol timeout.

Workaround: None.
- CSCsf27608

Symptom: Following an upgrade from Cisco SAN-OS 2.1(2b) to Cisco SAN-OS 3.0(2), a VSAN carrying FICON traffic was not trunking and the remote Domain Manager was not responding.

Workaround: None.
- CSCsf30937

Symptom: On rare occasions following an upgrade from Cisco MDS SAN-OS 2.1(2b) to Cisco SAN-OS 3.0(2a), module configurations might be removed.

Workaround: Reload the affected modules and then reconfigure or copy the configurations for the affected interfaces to the switch.
- CSCsf96043

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

Workaround: None.
- CSCsf97117

Symptom: IVR commit complains that one or more remote switches are running Cisco SAN-OS Release 2.04a and earlier.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: Clear the IVR session on the that was locked, activate the correct IVR full zone set after confirming that it is the same in all switches, or IVR commit on that switch.

- 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.

- CSCsg05037

Symptom: Cisco Fabric Manager shows read-write community strings for other communities when a user is logged in with a read-only community string.

Workaround: None.

- CSCsg10555

Symptom: Congestion in a switch might happen after a Supervisor 2 switchover, due to a misconfiguration on the standby Supervisor 2 during a downgrade to Cisco SAN-OS Release 3.0(2) or Release 3.0(2a). If this occurs during an in-service downgrade to Cisco SAN-OS Release 3.0.2, you might experience port flaps resulting in traffic disruption.

Workaround: None.

- 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.

- CSCsg12096

Symptom: When in-order delivery (IOD) is disabled, an entry in the accounting log is posted showing that it is enabled.

Workaround: None.

- CSCsg13769

Symptom: The management port link status LED on the Supervisor-2 module might not display the current status.

Workaround: None.

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsg18834

Symptom: When an IBM mainframe using FICON issues a 32 command to read port statistics, the MDS switch does not respond correctly. The host never clears allegiance which results in the customer being unable to do FICON management, either through Device Manager or the CLI, on the switch itself. If the host continues to periodically send the 32 command to the Control Unit Port (CUP) device, the ficonstat process can run out of memory and can result in supervisor switchover.

Workaround: Perform a system switchover.
- CSCsg19198

Symptom: If you use Fabric Manager to log on to a Cisco MDS 9000 switch with AAA authentication configured, you might see an error message saying that a maximum of 16 CLI sessions have been reached on the switch.

Workaround: Close some of the existing Fabric Manager or Device Manager sessions.
- 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.
- CSCsg41556

Symptom: Following an upgrade from Cisco SAN-OS 2.0(2b) to Cisco SAN-OS 3.0(2) on a switch where Fabric Binding is enabled, the switch displays this message:

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

Fabric Binding incorrectly causes the ENTERPRISE_PKG to start the grace period even if Fabric Binding is being used solely for FICON VSANs under the installed MAINFRAME_PKG license.

Workaround: Although there is no workaround for this issue, you can use the **show license usage ENTERPRISE_PKG** command to verify that Fabric Binding is using the ENTERPRISE_PKG license.
- CSCsg52197

Symptom: After you install an MPS-14/2 module, the power capacity level on the switch might be incorrect.

Workaround: To correct the power capacity level, switch the power capacity from Redundant to Combined and then back to Redundant again.
- 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.
- CSCsg80637

Symptom: Files placed on the volatile: partition cannot be copied or viewed by a user with the network-admin role.

Workaround: Log in to the MDS switch. with the same user that created the file and view or copy the file from the volatile partition.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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:
- CSCsg94749

Symptom: If an MDS switch running Cisco SAN-OS 3.0(x) is configured so that the default gateway is on the FCIP network and there is a static route for the management LAN, then the FCIP tunnel might go down.

Workaround: Configure the default gateway on the management LAN and a static route for the FCIP tunnel.
- CSCsg96497

Symptom: Following an upgrade to Cisco SAN-OS 3.x in a chassis where Generation 2 modules are present and FC flows are present, if you create and delete FC flows several times, then FC flows might not be able to be created anymore. You might see the following message in Fabric Manager when you click **Finish after** creating an FC flow:

```
Snmp: acltcam: Unable to allocate memory
```

Workaround: To resolve this issue, follow these steps:

 1. Reload each Generation 2 module, which is disruptive.
 2. Call TAC to obtain the debug plug-in to restart the ACL process, which is disruptive.
 3. Upgrade to Cisco SAN-OS 3.1(1).
- CSCsg99049

Symptom: Fabric Manager does not allow you to create more than 2048 flows per switch. The actual limitation is 2048 flows for a Generation 2 module and 1024 flows for a Generation 1 module.

Workaround: None.
- 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.
- CSCsh40033

Symptom: When a device is removed from remote switch, the device might still appear in the name server database, and the **fcns refresh** command might fail to remove the stale entry.

Workaround: To remove the state entry from the name server database, follow these steps:

 1. Connect a device on the remote switch which is not part of the active zone set.
 2. Apply the **refresh fcns** command required by Cisco.
 3. Use the **show fcns database** command to verify that the stale entry was removed.
 4. Shut down the new device or add it to the active zone set if needed.
- CSCsh66010

Symptom: If the limit of 5000 iSCSI sessions is reached and new initiators try create sessions, a memory leak may occur.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: Do not exceed the 5000 session limit.

- 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.

- CSCsi27133

Symptom: If an interface index map is not programmed correctly, the Port Manager continues to bring up the port, which results in an ACL programming failure and the following error message:

```
%ZONE-2-ZS_TCAM_PROGRAMMING_FAILED: %$VSAN xxx%$ TCAM operation failed : Unknown,
Reason: idxmap ioctl failure
```

Because of the programming failure, the port is effectively useless, even though it is up.

Workaround: None.

- CSCsj07363

Symptom: An SNMP Get-Next Request for the MIB object `ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex` on an MDS 9000 switch resolves by asking `ifIndex` for a loopback address. Because there is no hardware (`ifIndex`) for a loopback address, the `ifIndex` reply for this interface is skipped and the next possible instance of the object, which is `IP-MIB::ipAdEntNetMask`, is returned.

Workaround: There are two ways you can work around this issue. Do one of the following:

- Use the CISCO-IP-IF-MIB, which has richer vocabulary than the standard MIB. The same information along with more details can be derived.
- Use the Get-Next request in a series for `ipAdEntAddr` to learn about the all the address instances. Then do a series of specific Get Request requests for respective instances of `ipAdEntIfIndex` and ignore the loopback address.

- 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.

- CSCsg31334

Symptom: When you create a user with the name `user`, only the `snmp-user` is created and not the corresponding CLI user. There is no warning message about this.

Workaround: None.

- CSCeh35635

Symptom: For passwords authenticated by an AAA server, the MDS switch should inform the user when their password is about to expire.

Workaround: This is an enhancement. It is available only for CLI logins. Fabric Manager and Device currently do not support this feature.

- CSCsd92433

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

Send documentation comments to mdsfeedback-doc@cisco.com

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*

Send documentation comments to mdsfeedback-doc@cisco.com

- *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

Send documentation comments to mdsfeedback-doc@cisco.com

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>

Send documentation comments to mdsfeedback-doc@cisco.com

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>

Send documentation comments to mdsfeedback-doc@cisco.com

- 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/abtnicd/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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Send documentation comments to mdsfeedback-doc@cisco.com

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.