

Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.3(4a)

Release Date: April 19, 2004

Text Part Number: OL-4959-05 Rev. U0

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 27.



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 Note*:
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 On-Line Change History

Revision	Date	Description
A0	8/11/2004	Added DDTS CSCed44067 .
B0	8/26/2004	Added a limitation about Upgrading to Release 1.3(3) .
C0	9/2/2004	Added DDTS CSCee44707 and CSCed64425 .
D0	9/15/2004	Added DDTS CSCee51071 .
E0	11/09/2004	Added DDTS CSCef83504 .
F0	11/17/2004	Added DDTS CSCeg23889 and image upgrade references.
G0	12/3/2004	Added DDTS CSCee01143 .
H0	12/08/2004	Added DDTS CSCin81760 .
I0	12/22/2004	Added DDTS CSCeg61535 .
J0	01/14/2005	Added DDTS CSCeg56197 .
K0	01/21/2005	Modified DDTS CSCee06496 .



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 1 On-Line Change History (continued)

Revision	Date	Description
L0	02/22/2005	Added DDTS CSCee83961 , CSCee89946 , CSCef06657 , CSCee95629 , CSCin74613 , CSCee04343 , CSCee79377 , CSCee54650 , CSCef21105 .
M0	03/24/2005	Removed DDTS CSCdz12179 . Resolved in previous release. Added DDTS CSCed20053 , CSCee43249 , CSCef65409 , CSCef70000 , CSCeg13762 , CSCeg18886 , CSCeh21199 .
N0	05/31/2005	Added DDTS CSCeh42252 and CSCeg66225 .
O0	06/23/2005	Added DDTS CSCei25319 .
P0	07/29/2005	Added DDTS CSCed57251 , CSCeh61610 , and CSCec31365 .
Q0	08/22/2005	Removed DDTS CSCeh61610 .
R0	08/23/2005	Added DDTS CSCeh61610 .
S0	05/01/2006	Added DDTS CSCeg84871 , CSCei91676 , CSCej08751 , and CSCsc33788 .
T0	06/06/2006	Removed DDTS CSCed16845 .
U0	02/26/2007	Added DDTS CSCsh27840 .

Contents

This document includes the following section:

- [Introduction, page 3](#)
- [System Requirements, page 4](#)
- [Image Upgrade, page 6](#)
- [New Features in Release 1.3\(4a\), page 6](#)
- [Limitations and Restrictions, page 12](#)
- [Caveats, page 14](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation, page 28](#)
- [Documentation Feedback, page 29](#)
- [Cisco Product Security Overview, page 29](#)
- [Obtaining Technical Assistance, page 30](#)
- [Obtaining Additional Publications and Information, page 32](#)

Send documentation comments to mdsfeedback-doc@cisco.com

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offers intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. These switches combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

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

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 1.3(4a) and includes the following topics:

- [Hardware Supported, page 4](#)
- [Determining the Software Version, page 5](#)

Hardware Supported

Table 2 lists the hardware components supported on the Cisco MDS 9000 Family.

Table 2 Cisco MDS 9000 Family Supported Hardware Modules

Component	Part Number	Description	Applicable Products
Software	M95S1K9-1.3.4	MDS 9500 Series supervisor/fabric-I, enterprise software	MDS 9500 Series only
	M92S1K9-1.3.4	MDS 9216 enterprise software	MDS 9216 only
	M91S1K9-1.3.4	MDS 9100 Series enterprise software	MDS 9100 Series only
Chassis	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 sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately)	MDS 9216 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
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports)	MDS 9140 only
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 supervisor/fabric-I, module	MDS 9500 Series only
Switching modules	DS-X9016	MDS 9000 16-port 2/1-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9216
	DS-X9032	MDS 9000 32-port 2/1-Gbps Fibre Channel module (SFPs sold separately)	
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP storage services module.	
	DS-X9304-SMIP	4-port Gigabit Ethernet IP storage services module.	
	DS-X9032-SMV	32-port Fibre Channel Advanced Services Module (ASM).	
	DS-X9560-SMC	Caching Services Module (CSM)	

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

Table 2 Cisco MDS 9000 Family Supported Hardware Modules (continued)

Component	Part Number	Description	Applicable Products
LC-type fiber-optic SFP ¹	DS-SFP-FC-2G-SW	2/1-Gbps Fibre Channel — short wave SFP	MDS 9000 Family
	DS-SFP-FC-2G-LW	2/1-Gbps Fibre Channel — long wave SFP	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel—short wave SFP	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel — long wave SFP	
CWDM ²	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 2/1-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s)	
Power supplies	DS-CAC-300W	300W AC power supply	MDS 9100 Series only
	DS-CAC-845W	845W ³ AC power supply	MDS 9216 only
	DS-CAC-2500W	2500W AC power supply	MDS 9509 only
	DS-CDC-2500W	2500W DC power supply	
	DS-CAC-4000W-US	4000W AC power supply for US (cable attached)	MDS 9506 only
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CAC-1900W	1900W AC power supply	
	DS-CDC-1900W	1900W DC power supply	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB	MDS 9500 Series only
Port analyzer adapter	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
	DS-PAA-2		

1. SFP = small form factor pluggable
2. CWDM = coarse wave division multiplexing
3. W = Watt

Determining the Software Version



Note

We strongly recommend that you use the latest available software release for all Cisco MDS 9000 Family products.

To determine the version of the Cisco SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log into the switch and enter the **show version EXEC** command.

To determine the version of the Cisco 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)

Image Upgrade

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.

You can nondisruptively upgrade to (or downgrade from) Release 1.3(4a) using any Cisco MDS SAN-OS software release other than Release 1.0(2a).

**Note**

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

New Features in Release 1.3(4a)

SAN-OS Release 1.3(4a) is a maintenance release for switches in the Cisco MDS 9000 Family. See the “[Caveats](#)” section for details on closed and outstanding caveats and limitations.

**Note**

The *Release Notes* are specific to this maintenance release. For 1.3 documentation, see the “[Related Documentation](#)” section on page 27).

The following new features are introduced in Release 1.3(4a):

- “[IPS-4 Module](#)” section on page 6
- “[License Enforcement](#)” section on page 7
- “[FICON](#)” section on page 7
- “[Online Health Management System](#)” section on page 8
- “[IP Storage Updates](#)” section on page 8
- “[In-Order Delivery Per-VSAN Option](#)” section on page 9
- “[Zone Aliases](#)” section on page 8
- “[Distributing Zonesets at the EXEC Level](#)” section on page 9
- “[Adding and Withdrawing IVR Domains](#)” section on page 10
- “[New CLI Commands](#)” section on page 10
- “[Deprecated CLI Commands](#)” section on page 10
- “[Port Analyzer Adapter 2](#)” section on page 10
- “[Cisco MDS 9000 Family Fabric and Device Manager Updates](#)” section on page 10
- “[CSM Backward Compatibility](#)” section on page 12

IPS-4 Module

Effective Release 1.3(4a) the 4-port, hot-swappable IPS (IPS-4) modules are available for use in any Cisco MDS 9216 Switch or any switch in the Cisco MDS 9500 Series. Each of the four Gigabit Ethernet ports in this module can be configured to support FCIP protocol, iSCSI protocol, or both protocols simultaneously.

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

Refer to the *Cisco MDS 9216 Switch Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide* for further information.

The software configuration options remain the same as the IPS-8 module. Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

License Enforcement



Caution

While Release 1.2(x) and earlier did not enforce licenses, any future software upgrade will enforce license requirements and the grace period.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Obtaining License Key Files

If you already have a switch and would like to install the license yourself, you must obtain a license key file.

SAN_EXTN_OVER_IP_IPS4 License

The IPS-4 module is available with a new license, SAN_EXTN_OVER_IP_IPS4.

Grace Period Increased to 120 Days

Effective Release 1.3(4a), the grace period has been increased to 120 days.

FICON

The FICON feature is available in all Cisco MDS 9000 Family Switches in Release 1.3.

Refer to the *Cisco MDS 9000 Family Interoperability Support Matrix* for supported FICON configurations.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Port Numbering

In Release 1.3(4a), the port numbering schemes begins with a zero (0) instead of one (1). FCIP and PortChannels cannot be used in a FICON-enabled VSAN unless they are explicitly bound to a port number.

First Available Port Numbers

Use the **show ficon first-available port-number** command to find the first available port number to bind a FCIP or PortChannel interface.

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

Moving a FICON VSAN to an Offline State

Use the EXEC-level **ficon vsan vsan-id offline** command to log out all ports in the VSAN that needs to be suspended.

Use the EXEC-level **ficon vsan vsan-id online** command to remove the offline condition and to allow ports to log on again.

Online Health Management System

The Online Health Management System (OHMS) is a hardware fault detection and recovery feature. It ensures the general health of switching, services, and supervisor modules in any switch in the Cisco MDS 9000 Family effective SAN-OS Release 1.3(4a) and later.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Zone Aliases

Effective Release 1.3(4a), the SAN-OS software supports a maximum of 2048 aliases per VSAN.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

IP Storage Updates

The changes and updates to the IP storage configuration options are identified in this section.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Enabling iSCSI or FCIP

In Releases 1.3(2a) and 1.3(3), the IPS Gigabit Ethernet ports do not start functioning automatically until either the iSCSI feature or the FCIP feature is enabled. You can enable iSCSI by issuing the **enable iscsi** command. You can enable FCIP by issuing the **enable fcip** command.

Effective Release 1.3(4a), this is no longer a requirement—you can configure IP connectivity to a Gigabit Ethernet interface without enabling either the iSCSI feature or the FCIP feature.

Refer to [CSCed94302](#) for further information.

FCC Support

Effective Release 1.3(4a), FCC is supported on Cisco MDS switches with IPS modules. By default, the FCC protocol is disabled. FCC must be enabled for the entire switch and for all switches in the fabric. Each IPS module can only have 10 configured pWWNs per initiator, 1600 sessions, and 800 iSCSI hosts.

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

FCIP Defaults

Effective Release 1.3(4a), the default for the FCIP **tcp min-available-bandwidth** command is 500 Mbps.

iSCSI Defaults

Effective Release 1.3(4a), the iSCSI TCP parameters have the following changes.

- The default for the iSCSI **tcp send-buffer-size** command is 4096 KB.
- The default for the iSCSI **tcp min-available-bandwidth** command is 70 Mbps.

Burst Size for iSCSI Interfaces

The congestion window monitoring (CWM) option determines the maximum burst size allowed after an idle period. This option is now available for iSCSI interfaces effective Release 1.3(4a).

By default, the iSCSI **tcp cwm** option is enabled and the default burst size is 50 KB. The valid range is 10 to 100 KB.

Delay Jitter Estimation

A new TCP feature is added for both iSCSI and FCIP interfaces to obtain a round trip variation in the window size that can achieve maximum bandwidth.

Effective Release 1.3(4a), the **tcp max-jitter** command is available to estimate the maximum delay jitter experienced by the sender in microseconds and the default value is 100 microseconds for FCIP and 500 microseconds for iSCSI interfaces. The estimated variation should not include network queuing delay.

In-Order Delivery Per-VSAN Option

Effective Release 1.3(4a), the in-order delivery (IOD) feature can be enabled for specific VSANs. This feature is disabled by default in all Cisco MDS switches and can be enabled for the entire switch or individual VSANs as required.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Distributing Zonesets at the EXEC Level

Effective Release 1.3(4a), you can use the **zoneset distribute vsan vsan-id** command in EXEC mode to configure the Cisco MDS switch to distribute inactive, unmodified zonesets throughout the fabric. This command distributes the full zoneset information immediately.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

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

Adding and Withdrawing IVR Domains

The **ivr virtual-fcdomain-add** command enables all IVR virtual domains that are currently present in the fabric (and any virtual domain that is created in the future) to appear in the assigned domain list for the specified VSAN.

You can also temporarily withdraw overlapping virtual domains from a specific VSAN using the **ivr withdraw domain** command in EXEC mode.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

New CLI Commands

Besides the commands that address the new features listed above, the following new commands are added to the SAN-OS software in Release 1.3(4a):

- Use the **show tech-support brief** command to obtain a quick, condensed review of your switch configurations.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

Deprecated CLI Commands

The following commands are deprecated in Release 1.3(4a):

- **show fcip portnumber** (replaced by **show ficon first-available port-number**)
- **copy file startup-config** (the startup configuration can only be copied to NVRAM not from NVRAM)

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

Port Analyzer Adapter 2

Effective Release 1.3(4a), the Cisco MDS 9000 Family Port Analyzer Adapter 2 (PAA-2) provides solutions which work in conjunction with the Switched Port Analyzer (SPAN) feature on switches in the Cisco MDS 9000 Family.

Refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note* for further information

Cisco MDS 9000 Family Fabric and Device Manager Updates

In SAN-OS release 1.3(4a) Device Manager is updated with the following:

- Added:
 - Show Cores to Admin menu.
 - Diagnostics to Interface menu.
 - Ethernet and iSCSI to Interface menu.
 - Hardware to Logs menu.
 - Events to Logs menu.

Send documentation comments to mdsfeedback-doc@cisco.com

- Accounting to Logs menu
- Link Incidents to Logs menu.
- A syslog server to generate the Hardware, Events, Accounting, and Link Incidents logs.
- Moved -
 - System from Admin to Physical menu.
 - TCP/UDP from IP to Interface>Mgmt menu.
 - IPFC from IP to Interface>Mgmt menu.
 - WWN Manager from FC to FC>Advanced menu.
 - FCS from FC to FC>Advanced menu.
 - FDMI from FC to FC>Advanced menu.
 - LUNs from FC to FC>Advanced menu.
 - FSPF from FC to FC>Advanced menu.
 - Routes from FC to FC>Advanced menu.
 - FCC from FC to FC>Advanced menu.
 - Flow Statistics from FC to FC>Advanced menu.
- Changed:
 - FICON interface significantly from prior (preliminary) releases.

In SAN-OS release 1.3(4a) Fabric Manager is updated with the following:

- Added:
 - Switches>Interfaces>Management.
 - Ability to create Fibre Channel alias for switch ports.
 - License wizard that replaces one-click install dialog.
 - iSCSI wizard.
 - Step to FCIP wizard to show minimum/maximum bandwidth, estimated roundtrip time, and for write acceleration and compression settings.
- Moved:
 - Port Security from All Vsans to individual VSAN folders in Logical tree.
 - QoS from Switches to Switches>FC in Physical tree.
 - Port Channels from Switches to Switches>Interfaces in Physical tree.
 - FC Physical from Switches>FC to Switches>Interfaces in Physical tree.
 - FC Logical from Switches>FC to Switches>Interfaces in Physical tree.
 - SVC from Switches>FC to Switches>Interfaces in Physical tree.
 - IPFC from Switches>IP to Switches>Interfaces>Management in Physical tree.

Send documentation comments to mdsfeedback-doc@cisco.com

- Combined:
 - Name Server, RSCN from All VSANs under All VSANs>Advanced folder in Logical tree.
 - Name Server, RSCN from individual VSAN folders under VSAN>Advanced folders in Logical tree.
 - GigE, EtherChannels from Switches>IP>Physical Interfaces under Switches>Interfaces>Ethernet in Physical Tree.
- Changed:
 - Services other than Cisco Fabric Manager to be installed during first use of an associated feature.

Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* for further information.

CSM Backward Compatibility

The CSM is compatible with SAN-OS Release 1.3.1 and above. If you need to downgrade to a release earlier than 1.3(1), you must power off the CSMs before performing the downgrade (see [CSCee69099](#)).

To revert to a release that is earlier than Release 1.3(1), follow these steps:

-
- Step 1** Power down all CSMs using the **poweroff module slot** command.
 - Step 2** Remove any CSMs related configuration (for example, clusters, back-end storage, virtual disks, and so forth).

Refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*.
 - Step 3** Save the configuration using the **copy running-config startup-config** command to save the new configuration into nonvolatile storage.
 - Step 4** Continue with the manual downgrade procedure.

Refer to Chapter 5, “Software Images” in the *Cisco MDS 9000 Family Configuration Guide*.
-

Limitations and Restrictions

The following limitations and restrictions apply to all switches in the Cisco MDS 9000 Family:

- [Upgrading to Release 1.3\(3\), page 13](#)
- [Installing Multiple Licenses, page 13](#)
- [Moving Licenses Between Switches, page 13](#)
- [FCC Usage, page 13](#)
- [Deleting Files, page 13](#)
- [Distributing Unconditional Full Zone Sets, page 13](#)
- [Withdrawing IVR Domains, page 13](#)
- [Device Manager Loopback Diagnostics, page 14](#)
- [Fabric Manager License Status, page 14](#)

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

Upgrading to Release 1.3(3)

When upgrading to SAN-OS Release 1.3(3) from any earlier SAN-OS release, the upgrade may fail based on the type of Call Home options configured. Refer to [CSCed44067](#) for further information.

Remove all email address configurations for all destination profiles before performing the upgrade. Apply the Call Home configuration after the upgrade. Use the following command to remove the email address configurations.

```
switch(config-callhome)# no destination-profile profile-name email-addr email-address
```

Installing Multiple Licenses

If you need to install multiple licenses in any switch in the Cisco MDS 9000 Family, be sure to provide unique file names for each license key file.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

Moving Licenses Between Switches

A license is specific to the switch for which it is issued and is not valid on any other switch. If you need to transfer a license from one switch to another, contact your customer service representative.

Refer to the *Cisco MDS 9000 Family Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide* for further information.

FCC Usage

If a Caching Services Module (CSM) running Release 1.3(1) exists in the fabric, do not enable FCC for any switch in the fabric.

Deleting Files

The **delete** command deletes a specified file or the specified directory and all its contents.

If you specify a directory, the **delete** command deletes the entire directory and all its contents.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

Distributing Unconditional Full Zone Sets

The **zoneset distribute vsan vsan-id** command is supported in **interop 2** and **interop 3** modes—not in **interop 1** mode.

Withdrawing IVR Domains

Withdrawing an overlapping virtual domain from an IVR VSAN disrupts IVR traffic to and from that domain.

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

Device Manager Loopback Diagnostics

When Device Manager is operating with SAN-OS Release 1.3.4a, traffic is disrupted during an external loopback diagnostic test.

You must connect a cable (or a plug) to loop the Rx port to the Tx port before running the loopback test. During an external loopback test on the ports, all the ports are stepped through one at a time and are taken up or down momentarily causing traffic disruption.

There is no warning to say this is disruptive nor is there a option to select a port individually. This is a known defect and will be resolved in a future release.

Fabric Manager License Status

When your grace period license is within 30 days of expiring, you will see a “License Violation” error in the Status column within the Switches folder when Fabric Manager is running. You are not in violation of any license agreement. This message indicates that you are within 30 days of your license expiration date.

Caveats

This section lists the caveats and corrected caveats for this release. Use [Table 3](#) to determine the status of a particular caveat. In the table, “R” indicates a resolved caveat, and “O” indicates an open caveat.

Table 3 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release (Resolved or Open)	
	1.3(3c)	1.3(4a)
Severity 1		
CSCed44067	O	R
CSCee51071		O
CSCeg13762	O	O
Severity 2		
CSCed35356	O	R
CSCed42077	O	R
CSCed57251	O	O
CSCed65607	O	R
CSCed75825	O	R
CSCee01143	O	R
CSCee06496	O	R
CSCee30799		O
CSCee43249	O	O
CSCee69099		O
CSCee95629		O

Send documentation comments to mdsfeedback-doc@cisco.com

Table 3 Release Caveats and Caveats Corrected Reference (continued)

DDTS Number	Software Release (Resolved or Open)	
	1.3(3c)	1.3(4a)
CSCef00869		O
CSCef06657		O
CSCef65409		O
CSCef83504	O	O
CSCeg18886		O
CSCeg23889		O
CSCeg84871	O	O
CSCeh61610		O
CSCei25319	O	O
CSCin74613		O
CSCsh27840	O	O
Severity 3		
CSCea45726	O	R
CSCea82028	O	Non-issue
CSCec10009	O	R
CSCec31365	O	O
CSCed14360	O	R
CSCed14920	O	O
CSCed20053	O	O
CSCed31611	O	R
CSCed34922	O	Non-issue
CSCed35965	O	R
CSCed51574	O	R
CSCed58155	O	R
CSCed64425	O	R
CSCed94302	O	R
CSCed96246	O	R
CSCee02629		R
CSCee04343	O	O
CSCee26227		O
CSCee28076		O
CSCee34199		O
CSCee38287		O
CSCee44707		O
CSCee54650	O	O

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

Table 3 Release Caveats and Caveats Corrected Reference (continued)

DDTS Number	Software Release (Resolved or Open)	
	1.3(3c)	1.3(4a)
CSCee79377		O
CSCee83961		O
CSCee89946	O	O
CSCef06657		O
CSCef21105		O
CSCef70000		O
CSCeg56197	O	O
CSCeg61535	O	O
CSCeg66225	O	O
CSCeh21199	O	O
CSCei91676	O	O
CSCej08751	O	O
CSCin81760	O	O
CSCsc33788		O
Severity 4		
CSCeh42252	O	O

Resolved Caveats

- [CSCed44067](#)

Symptom: When upgrading to Cisco MDS SAN-OS Release 1.3(3) from any earlier release, the upgrade may fail based on the type of CallHome options configured.

Workaround: Remove all email address configurations for all destination profiles before performing the upgrade. Apply the Call Home configuration after the upgrade. Use the following command to remove the email address configurations.

```
switch(config-callhome)# no destination-profile profile-name email-addr email-address
```

- [CSCed35356](#)

Symptom: When configuring the nWWN for an iSCSI initiator using the Device Manager, you may encounter a `NullPointerException` error.

Workaround: None.

- [CSCed42077](#)

Symptom: When a McData switch with firmware 4.01.xx/5.01.xx/5.02.xx in open-fabric mode is attached to a Cisco MDS switch and the hosts attached to the MDS register a symbolic port or node name with the FCNS, the name server on the McData switch may send abort sequences to devices that are locally attached to the McData switch. According to the FC-SW2 spec, (Section 9.3.3 Name Server Objects), Port Symbolic Name and Node Symbolic Name are not mandatory fields in the

Send documentation comments to mdsfeedback-doc@cisco.com

small name server object. The result is that an end device that successfully registers a symbolic Port/Node name with an MDS switch may cause the McData switch name server to malfunction and send abort sequences to end devices that log into the McData name server.

Workaround: Plug all devices that register symbolic node/port world wide names into the McData. This issue exists as of Cisco MDS firmware up to and including 1.3(3c).

- CSCed65607

Symptom: A vulnerability in the Transmission Control Protocol (TCP) specification (RFC 793) was discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the attacked protocol, a successful attack may have additional consequences beyond terminated connection. This attack vector is only applicable to those sessions terminating in a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at the following website, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

Workaround: Depending on the application, the connection may get automatically reestablished. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session).

- CSCed75825

Symptom: If a spare supervisor module has the local boot variables pointing to Release 1.0(1) or 1.0(2) images, inserting that spare supervisor module into a functioning switch will cause the active supervisor module to fail. This issue exists in all releases up to and including Release 1.3(3c).

Workaround: If the active supervisor runs any of the affected releases, check the version of the spare supervisor module before inserting it, or issue the **reload module slot-number force-dnld** command immediately after the insertion. The *slot-number* is the number of the slot in which the spare module is inserted.

- CSCee01143

Symptom: You may not be able to login to Fabric Manager or Device Manager using SNMPv3. You may get the following error message:

```
SNMP NotInTimeWindow
```

Workaround: Set the clock on the switch to a different value and then set it to your correct time. For Example.

```
MDS# clock set 04:23:01 26 March 2000
```

```
MDS# clock set 04:23:01 11 November 2004
```

After setting the clock, launch FM and verify the connection.

- CSCee06496

Symptom: If you are running Cisco MDS SAN-OS releases 1.1(3), 1.2(1a), 1.2(1b), 1.2(2a), 1.3(1), 1.3(2a), 1.3(3), or 1.3(3c), the following sequence of operations might lead to the failure of one or both supervisor modules simultaneously:

- Removing an IPS-8 module from the switch.
- Inserting a different type of module in the same slot.

Send documentation comments to mdsfeedback-doc@cisco.com

- c. Configuring the new module.
- d. Issuing the **copy running-config startup-config** command.

Removing the IPS-8 module at any time and replacing with another IPS-8 module does not cause this problem.

Workaround: Before replacing an IPS-8 module with a different type of module in the same slot, upgrade to Cisco MDS SAN-OS Release 1.3(4a).

- CSCeh61610

Symptom: FCIP Write Acceleration does not work with certain storage replication subsystems.

Workaround: None.

- CSCei25319

Symptom: An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to a SNMP query. In some cases, this results in the query not being responded to.

Workaround: Perform a refresh on Device Manager to clear the problem.

- CSCea45726

Symptom: The Device Manager shows a port in the down state (red square) when the operational status of the port is up. This rare occurrence is due to the failure cause of the port not being empty (for example, the failure case reflects the `initializing` state).

Workaround: None.

- CSCea82028

Symptom: When a switch is upgraded while the Device Manager for that switch is open, a Java error of class cast exception occurs. When this error occurs, some Device Manager menu items are unusable while other menu items remain in this error state.

Workaround: Close the Device Manager and reopen it.

- CSCec10009

Symptom: When a previously-connected port is disconnected and reconnected to a different port, the old port connection displays a red cross. The tool tip continues to show the presence of the new port and the old port as members of the loop. When this happens the WWN of the new device is both in the tool tip of the nonexistent loop and in the disconnected device. It may take a poll cycle for the PortChannel to appear on the fabric map.

Workaround: Refresh or purge the fabric map to remove the nonexistent (dead) link.

- CSCec31365

Symptom: When IVR is enabled, the Fabric-Device Management Interface information is not transferred across VSANs for IVR devices.

Workaround: None.

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

- CSCed14360

Symptom: If a switch does not have sufficient PortChannels available for an SVC Interface, it will remain in a failure state. This situation can occur if you allocate all 128 PortChannels available in the system. You can verify this failure if you see the `node down` status in the output of the **show interface svc slot/node** command. To confirm that this failure is a result of insufficient PortChannels, issue the **show port-channel usage** command.

Workaround: Identify at least three PortChannels that can be released so they appear in the unused section of the **show port-channel usage** command output. Use the **no interface port-channel number** command to delete unneeded PortChannels. Finally, reset the SVC Interface.
- CSCed31611

Symptom: Due to an internal error, the `fcFxpPortID` returns a wrong FCID value from the FIBRE-CHANNEL-FE-MIB.

Workaround: None.
- CSCed34922

Symptom: The Fabric Manager map layout is not preserved when the FC domain is restarted.

Workaround: None—This is a non-issue for Release 1.3(4a)
- CSCed35965

Symptom: Using a script to send Common Information Model (CIM) queries via the CIM Pegasus CLI client may result in a memory leak.

Workaround: None. The CIM server automatically reinitializes on detecting a memory leak.
- CSCed51574

Symptom: When you issue the **show fcalias vsan vsan-id** command, the switch may sometimes remain in the hung state for an indefinite period.

Workaround: Enter **Control-c** to exit the hung state and then issue the **show running-config** command at the switch prompt to see the available aliases.
- CSCed58155

Symptom: The Fabric Manager (FM) cannot correlate an iSCSI host with two NIC cards when the iSCSI initiator is identified by the IP address (either from a matching static **iscsi initiator ip-address** command or from an iSCSI interface **switchport initiator id ip-address** command for dynamic initiators). This is a result of the switch putting IP address in the symbolic-node-name field in the FCNS entry for that initiator. This was done to allow zoning based on IP address in ISAN software Release 1.1(x) and 1.2(x) where zone membership for iSCSI initiator can only be based on symbolic-node-name value.

Workaround: To allow FM to show the above-mentioned host properly, the switch will instead fill the FCNS entry's symbolic-node-name field with the actual iSCSI initiator node name (i.e. its IQN name).

This impacts for users who configure zoning based on iSCSI initiator's IP address via the symbolic node name field, e.g.

```
zone name a vsan 1
member symbolic-nodename 10.2.2.112
```

Change the above configuration to the following for this configuration to continue working after upgrading to Release 1.3(4a).

```
zone name a vsan 1
member ip-address 10.2.2.112
```

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCed64425

Symptom: You can TFTP to a Cisco MDS switch through the management interface from any TFTP client. In SAN-OS Releases 1.3(4a), 1.3(4b) and 1.3(5), a default IP access control list (ACL) rule is added to block frames for ports like TFTP, SUNRP and BOOTP.

Workaround: For Cisco MDS SAN-OS Releases 1.2(1a), 1.2(1b), 1.2(2a), 1.3(1), 1.3(2a), 1.3(3), and 1.3(3c), manually create the drop rule by issuing the following commands in succession:

```
switch(config)# ip access-list abc deny udp any any eq port 69
switch(config)# ip access-list abc permit ip any any
switch(config)# interface mgmt 0
switch(config-if)# ip access-group abc
```
- CSCed94302

Symptom: Effective Release 1.3.x, despite assigning an IP address to a Gigabit Ethernet interface on a IPS module and enabling that interface (using the **no shutdown** command), a **ping** command to the interface's IP address is not answered.

Workaround: You must explicitly enable either FCIP or iSCSI using the **enable fcip** or **enable iscsi** commands.
- CSCed96246

Symptom: A new vulnerability in the OpenSSL implementation for SSL was announced on March 17, 2004. An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack.

Workaround: Refer to the following URL for further information:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_technical_reference09186a008020fd0e.html
- CSCee02629

Symptom: The IPS-4 module is released with Cisco MDS SAN-OS Release 1.3(4a). When you attempt to downgrade a switch from Cisco MDS SAN-OS Release 1.3(4a) or higher to Cisco MDS SAN-OS Release 1.3(3), and that switch has an IPS-4 module, then the downgrade fails for the IPS-4 module in this switch. This problem is specific to downgrading to release 1.3(3) in a switch with IPS-4 module.

Workaround: Power down the IPS-4 module before attempting to downgrade from Cisco MDS SAN-OS Release 1.3(4x) to Release 1.3(3).

Open Caveats

- CSCee51071

Symptom: A nondisruptive software upgrade/downgrade between Cisco MDS SAN-OS Release 1.3(4a) and Release 1.3(4b) fails when started from the Fabric Manager application due to an SNMP error. This problem is only a result of the SNMP agent and not of the Fabric Manager application.

Workaround: Use the command-line interface (CLI) to upgrade/downgrade from Release 1.3(4a) to Release 1.3(4b). Do not use the Fabric Manager to downgrade/upgrade software between these software versions.
- CSCeg13762

Symptom: A license installation failure occurs on the Cisco MDS 9216A switch running Cisco SAN-OS software releases 1.3(2a), 1.3(4a) and 1.3(5).

Send documentation comments to mdsfeedback-doc@cisco.com

- Workaround:** Upgrade to Cisco SAN-OS software releases 1.3(6), 2.0(1b) or later for successful license installation. If desired, the Cisco MDS 9216A switch can then be downgraded to releases 1.3(2a), 1.3(4a), or 1.3(5).
- CSCed57251

Symptom: In some rare instances in Cisco MDS SAN-OS Release 1.3, 2.0, and 2.1(1), when the IP Storage Services (IPS) module restarted after a failure, VSAN membership information about iSCSI interfaces was lost. However, a configuration saved with the **copy running-config startup** command was not lost.

Workaround: None.
 - CSCee30799

Symptom: If you add routes to new switches while in **interop** mode and later move the switch back to the default mode, then further updates to the FSPF database are not sent to the new switches and routes are lost to these switches after one hour.

If a switch is just in default mode or just in **interop** mode, this problem does not arise. It only arises if you move from the **interop** mode to the default mode in an active VSAN.

Workaround: Perform one of the following workarounds on each switch which was moved from the interop mode to default mode

 - Suspend and unsuspend the VSAN using the **vsan vsan-id suspend** and the **no vsan vsan-id suspend** commands
 - Disable and enable FSPF on the VSAN using the **no fspf enable vsan vsan-id** and the **fspf enable vsan vsan-id** commands.
 - CSCee43249

Symptom: If a malfunctioning device does not swap the source and destination FCIDs, a PLOGI frame sent by this device can cause high CPU utilization. These PLOGI frame errors are reported by the zone server.

Workaround: None.
 - CSCee69099

Symptom: If your current configuration is using CSMs and you need to downgrade from Release 1.3(1) or later to any release that is earlier than Release 1.3(1), do not issue the **install all** command before powering off the CSM(s).

Workaround: Explicitly power off the CSM before issuing the **install all** command. The CSM was only introduced in Cisco MDS SAN-OS Release 1.3(1). See the [“CSM Backward Compatibility” section on page 12](#)
 - CSCee95629

Symptom: After a Cisco MDS switch is power cycled, in some cases, the VRRP state of the IPS interfaces remains in the init state.

Workaround: Issue the shutdown command followed by the no shutdown command for the impacted interface to restart the VRRP state machine
 - CSCef00869

Symptom: Some sessions on the iSCSI host remain in reconnecting state after the host or the switch is rebooted.

Workaround: Manually log off and log on to the switch.

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

- CSCef06657
Symptom: If a host is connected to a Cisco MDS switch that is also connected to a loop (FL/NL port) and the loop goes down, an RSCN is sent to the host and the host performs a name server query. Even if the port is down, the name server continues to respond with the port ID of the offline port.
Workaround: None.
- CSCef65409
Symptom: SNMP daemon crashes periodically on a Cisco MDS 9000 Family switch running Release 1.3(4a). Issue the **show process memory | include snmp** commands at regular intervals to show the pattern of a memory increase.
Workaround: Upgrade to Cisco MDS SAN-OS Release 1.3(6).
- CSCef83504
Symptom: The system does not recognize a CLI password containing the “\$” character.
Workaround: Change your password to a different string that does not include the “\$” character. For an admin user-account, you might have to perform the password-recovery procedure to reset the password.
- CSCeg18886
Symptom: If multiple “get all next” queries are sent before receiving a response from the first one, some queries might be dropped as they overwhelm the name server buffers. Some arrays do this to improve performance, resulting in dropped queries.
Workaround: Upgrade to Cisco MDS SAN-OS Release 1.3(6).
- CSCeg23889
Symptom: License warning notifications, either through Call Home or system messages, might occur in the following situations:
 - The grace period for a license package was triggered (a feature licensed by that license package had been used). Currently none of the features licensed by this license package are enabled.
 - The grace period for a license package expired. None of the features licensed by this license package are enabled.**Workaround:** None.
- CSCeg84871
Symptom: When an iSCSI initiator logs in to a Gigabit Ethernet port number 1 on an IPS module in slot 1, the switch sends a login response with the value of the Target Session Identifying Handle (TSIH) field set to zero (0), which is an iSCSI protocol violation. This situation can also occur when an iSCSI initiator logs in to Ethernet PortChannel number 1. The Qlogic iSCSI initiator may verify the TSIH value and reject it.
Workaround: None.
- CSCin74613
Symptom: The license file corrupts when it is saved to a local disk.
Workaround: None.
- 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.

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

- CSCed14920

Symptom: During a switch upgrade, a SVC node may not save its entire state under rare circumstances. This results in that node not being part of the cluster after the switch upgrade. Verify this symptom by issuing the **show nodes local** command at the `svc-config` prompt—the command output displays the following information:

 - The `cluster state` of the affected SVC node will be `unconfigured`.
 - The `node state` of the affected SVC node will be `free`.

Workaround: Manually remove the SVC node from the cluster and then add the node back into the cluster. Refer to *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for procedural details.
- CSCed20053

Symptom: On rare occasions, the **install license** command may fail due to the saved state of the switch configuration. This may occur after saving a remote configuration to the switch using the **copy remote-url start-up** command.

Workaround: Issue the **copy ru st** command. The **install license** command should work properly after that.
- CSCee04343

Symptom: If the SAN-OS `fc analyzer local display-filter` command is issued in configuration mode with prepended lengthy and intricate filtering strings, it may cause the actual analyzer process to terminate. There is no impact on the stability of the Cisco MDS switch. Configurations without lengthy display-filters work fine.

Workaround: None.
- CSCee26227

Symptom: If you are logging in to a switch through SSH and you have issued the **aaa authentication login default none** command, you must enter one or more key strokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

If you are logging in through Telnet, just press the **Enter** key when prompted for password.

Workaround: None.
- CSCee28076

Symptom: If the switch contains one or more IPS-4 modules with productID DS-X9304-SMIP and a downgrade is performed from Cisco MDS SAN-OS Releases 1.3(3c), 1.3(4), or 1.3(4a) to SAN-OS Releases 1.3(3), 1.3(2a), 1.3(2), or 1.3(1), the service platform will terminate abruptly during a SNMP query causing service disruption.

Workaround: It is necessary to physically remove all the IPS-4 modules with productID DS-X9304-SMIP prior to starting the downgrade. It is not sufficient to power down the module.
- CSCee34199

Symptom: When you issue commands relating to the SAN Volume Controller (SVC) interface and then issue the **copy** command, the switch may sometimes remain in the hung state for an indefinite period.

Workaround: Enter **Control-c** to exit the hung state, log out of the switch, relogin to the switch, and finally issue the **copy** command.
- CSCee38287

Send documentation comments to mdsfeedback-doc@cisco.com

Symptom: Users downloading Java Runtime Environment version 1.4.2_01 or earlier from the EMC Corporation™ website, will not have the necessary SSL authorization certificate to validate the one-click license installation process.

Workaround: Upgrade to Java Runtime Environment version 1.4.2_04 or higher.

- CSCee44707

Symptom: In some rare cases, duplicate ACKs sent from a host to an IP Storage (IPS) services port triggers a TCP fast retransmit even if the IPS port did not receive three consecutive, duplicate ACKs.

Workaround: None. This is an enhancement.

- CSCee54650

Symptom: Under rare circumstances, it is possible to lose the cluster IP address when the config node fails. This problem is fixed in Cisco MDS SAN-OS Release 1.3(5).

Workaround: For releases prior to Cisco MDS SAN-OS 1.3(5):

- Connect to the switch using the switch's management IP address
- Use the `svc-config` and `show nodes local` commands to verify that the config node of the required cluster is present in that switch.
- Use the `svc-config`, `cluster config cluster-name`, and `ip new-ip-address` commands to change the cluster IP address for the cluster to another random address.
- Change the cluster IP address back to the original IP address using the same steps defined in Step C.

- CSCee79377

Symptom: With an MDS translative loop (TL) port, the assignment of proxy ALPA to the same fabric-based target WWN may vary if the sequence of targets joining the fabric changes (for example, after a reboot). This causes problems for private HBAs in HP-UX systems that access more than one fabric-based (public) targets. This is because HP-UX builds device definitions (CxTxDx) based on the ALPA/loop ID.

Workaround: Only zone the private HBA with one target pWWN.

- CSCee83961

Symptom: Your SSH login may fail if you do not have a local user account on the switch and if you use remote AAA (RADIUS/TACACS+) server authentication. This problem is fixed in SAN-OS 1.3(5).

Workaround: For releases prior to SAN-OS 1.3(5), first login through Telnet. Subsequent SSH logins will function after the first Telnet login.

- CSCee89946

Symptom: This caveat applies to Release 1.1(1) up to, and including, Release 1.3(4b). The Fibre Channel port link reinitialization sequence triggered by a link down event does not succeed if the switching module is up for more than 248 days and the last shutdown command on that port was issued 248 days prior to the link failure. After the link-down event, the port remains in the link failure or not connected state as shown in the following command output:

```
switch# show interface fc2/1
fc2/1 is down (Link failure or not-connected)
```

Workaround: Issue the shutdown command, followed by the no shutdown command, on the affected port to bring the port back to link-up state as shown in the following command output:

```
switch# config t
switch(config)# interface fc2/1
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
switch(config)# shutdown
switch(config)# no shutdown
```

Issue the following commands to verify the module uptime.

```
switch# attach module 2
Attaching to module 2 ...
```

To exit type **exit**, to abort type **\$**.

```
module-2# show version
Software
  BIOS:      version 1.0.8
  system:    version 2.0(1) [build 2.0(0.139)]
  BIOS compile time:      08/07/03
  system compile Time:    10/25/2020 12:00:00
Hardware
  RAM 186668 kB
  bootflash: 125184 blocks (block size 512b)
  lc02  uptime is 11 days 18 hours 18 minute(s) 9 second(s)
```

Other notes:

- Any nondisruptive upgrade or downgrade resets the 248-day window.
- Once the shutdown and no shutdown commands are issued, it is good for another 248 days.
- If the switch has been up for a long time and the customer wants to connect new devices to the switch ports, then you may start with the shutdown and no shutdown commands on those ports.

- CSCef06657

Symptom: If a host is connected to a Cisco MDS switch that is also connected to a loop (FL/NL port) and the loop goes down, an RSCN is sent to the host and the host performs a name server query. Even if the port is down, the name server continues to respond with the port ID of the offline port.

Workaround: None.

- CSCef21105

Symptom: The Cisco MDS 9500 supervisor module did not send a gratuitous ARP for CSM cluster IP address. This caused the host to lose connectivity to the Cluster IP address during a supervisor switchover. This problem is fixed in Cisco MDS SAN-OS 1.3(5).

Workaround: For releases prior to Cisco MDS SAN-OS 1.3(5), decrease the ARP cache timeout or manually delete the ARP entry for CSM cluster IP address at the host.

- CSCef70000

Symptom: If you downgrade from Cisco MDS SAN-OS Release 1.3(5) to Release 1.3(4), then you might lose your per-VSAN in-order delivery configuration.

Workaround: Reconfigure your system with the per-VSAN in-order delivery configuration.

- CSCeg56197

Symptom: Configuring the CIM server certificate as listed below might cause your switch to crash.

- a. Create a self-certified key (xxxxxx.pem file) on an external server (we use a utility under Hi-Command).
- b. Enter **conf t** to enter configuration mode.
- c. Enter **cimserver certificate xxxxxx.pem** to install a certificate specified in the file named with a .pem extension.
- d. Enter **cimserver enablehttps** to enable HTTPS (secure protocol).
- e. Enter **cimserver enable** to enable the CIM server.

Send documentation comments to mdsfeedback-doc@cisco.com

f. Enter **Ctrl-z** to quit

Workaround: None

- CSCeg61535

Symptom: The Telnet server may not be disabled even if you disable it through setup. A telnet session will still work in the switch.

Workaround: Issue the **no telnet server enable** command in configuration mode to disable telnet after you login to the switch.

- CSCeg66225

Symptom: Password recovery might fail if you use the **copy <config-url> startup** command to save the switch configuration, or if you boot a system image that is older than the image you used to store the configuration and did not use the install all command. The following message might display in syslog or on the console during the process of password recovery.

```
<<%ASCII-CFG-2-ACFG_CONFIGURATION_APPLY_ERROR>>
```

Workaround: Issue the **write erase** command from the switchboot prompt.



Note Using the write erase command will erase the configuration. You must reapply the configuration, if externally stored, after the switch login.

- CSCeh21199

Symptom: If the NetApp file server appliance is configured as an initiator performing a Network Data Management Protocol (NDMP) backup, then the fabric login (FLOGI) process on the MDS switch might terminate because of excessive LSTS requests.

This might happen if your N port or NL port uses extended link services to manage and control a public remote loop. The NetApp file server appliance configuration uses these services, namely LSTS and LINIT, which are documented in the Fibre Channel standards compliance (FC-FLA standard) specification.

Workaround: Upgrade to Cisco MDS SAN-OS Release 2.0(4).

- CSCei91676

Symptom: If iSCSI virtual targets are configured with more than 50 LUN maps, then erroneous overlapping LUN map system messages appear when the iSCSI initiator is not allowed to log in to these iSCSI virtual targets.

Workaround: Limit the number of configured LUN maps for an iSCSI virtual target to fewer than 50 LUNs.

- CSCej08751

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

Workaround: None.

- CSCin81760

Symptom: In some rare cases, license features are disabled when the IP address on a management port is changed.

Workaround: None. Enable the license features again.

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

- CSCeh42252

Symptom: If you try to configure SSH key for any of the non-local user- accounts, in some rare cases you might see a core dump on standby.

Workaround: First delete the non-local user-account and create it again so that it becomes a local user-account. Then perform any type of configuration for that user-account. User should not perform configuration operations on non- local user-accounts. Non-local user-accounts can be created due to users getting authenticated using RADIUS/TACACS+ server.

- CSCsc33788

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

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

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

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

Workaround: There are two ways to address this issue:

- To non-disruptively upgrade all modules that are running the older software version, issue the **install module module-number image** command.
- To disruptively upgrade the modules, issue the **reload module module-number force-dnld** command, or reinstall the module.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents:

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family System Messages Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference Guide*

Send documentation comments to mdsfeedback-doc@cisco.com

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: <http://support.veritas.com/>

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/>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Send documentation comments to mdsfeedback-doc@cisco.com

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to mdsfeedback-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Send documentation comments to mdsfeedback-doc@cisco.com

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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>

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

Send documentation comments to mdsfeedback-doc@cisco.com

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *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>

- 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.

