

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.3(1)

Release Date: December 9, 2003

Text Part Number: OL-4959-01, Rev. P0

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 28.



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	9/2/2004	Added DDTS CSCed64425 .
B0	11/9/2004	Added DDTS CSCef83504
C0	12/4/2004	Added DDTS CSCee01143 .
F0	12/08/2004	Added DDTS CSCin81760
G0	12/22/2004	Added DDTS CSCeg61535
H0	01/21/2005	Modified DDTS CSCee06496
I0	02/22/2005	Added DDTS CSCee89946
J0	03/24/2005	Added workaround information for all resolved caveats. Added DDTS CSCec79467 , CSCed10846 , CSCed13757 , CSCed32729 , CSCed32729 , CSCed58155 , CSCed65607 , CSCed75825 , CSCed94302 , CSCee18613 , CSCee43249 , CSCeh21199 . Removed caveat CSCdz43106 , CSCeb10797 . Resolved in a previous release.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 1 On-Line Change History (continued)

Revision	Date	Description
K0	05/31/2005	Added DDTS CSCeh42252 and CSCeg66225
L0	06/23/2005	Added DDTS CSCei25319
M0	07/29/2005	Added DDTS CSCed57251 and CSCec31365
N0	05/01/2006	Added DDTS CSCeg84871 , CSCei91676 , and CSCej08751 .
O0	06/06/2006	Removed DDTS CSCed16845 .
P0	02/26/2007	Added DDTS CSCsh27840 .

Contents

This document includes the following section:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [Image Upgrade, page 5](#)
- [New Features in Release 1.3\(1\), page 5](#)
- [Limitations and Restrictions, page 16](#)
- [Caveats, page 19](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation, page 29](#)
- [Documentation Feedback, page 30](#)
- [Cisco Product Security Overview, page 31](#)
- [Obtaining Technical Assistance, page 31](#)
- [Obtaining Additional Publications and Information, page 33](#)

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offer intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They 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(1) and includes the following topics:

- [Hardware Supported, page 3](#)
- [Determining the Software Version, page 4](#)

Hardware Supported

[Table 2](#) lists the hardware components supported on the Cisco MDS 9000 Family and the minimum software version required. See the “[Determining the Software Version](#)” section on [page 4](#).

Table 2 *Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements*

Component	Part Number	Description	Applicable Products
Software	M95S1K9-1.3.1	MDS 9500 Series supervisor/fabric-I, enterprise software	MDS 9500 Series only
	M92S1K9-1.3.1	MDS 9216 enterprise software	MDS 9216 only
	M91S1K9-1.3.1	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-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

Table 2 *Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements (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)	
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CAC-1900W	1900W AC power supply	MDS 9506 only
	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

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 MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch, log in to the switch and enter the **show version EXEC** command.

[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(1) using any Cisco MDS SAN-OS software release other than Release 1.0(2a).

New Features in Release 1.3(1)



Caution

Cisco MDS SAN-OS Release 1.3(1) has been deferred, please use Cisco MDS SAN-OS Release 1.3(2a) or later.



Note

Cisco MDS SAN-OS Release 1.3(1) is a **limited availability release** for the Caching Services Module (CSM).

See the “[Caveats](#)” section on [page 19](#) for details on closed and outstanding caveats and limitations.

The following new features are introduced in Cisco MDS SAN-OS Release 1.3(1):

- “[The Caching Services Module](#)” section on [page 6](#)
- “[Optional 2 RU Shelf Bracket](#)” section on [page 7](#)
- “[Inter-VSAN Routing](#)” section on [page 7](#)
- “[Quality of Service](#)” section on [page 7](#)
- “[FICON](#)” section on [page 8](#)
- “[Fabric Binding](#)” section on [page 8](#)
- “[Registered Link Incident Report](#)” section on [page 8](#)
- “[Licensing](#)” section on [page 8](#)
- “[New Features for the Cisco Fabric and Device Manager](#)” section on [page 9](#)
- “[Common Information Model](#)” section on [page 9](#)
- “[Fabric-Device Management Interface](#)” section on [page 10](#)
- “[FC-SP DHCHAP](#)” section on [page 10](#)
- “[TACACS+ Authentication](#)” section on [page 10](#)
- “[RADIUS Enhancements](#)” section on [page 10](#)
- “[AAA Server Groups](#)” section on [page 11](#)
- “[FCIP Write Accelerator](#)” section on [page 11](#)
- “[FCIP Compression](#)” section on [page 11](#)
- “[Proxy Initiator](#)” section on [page 11](#)
- “[Trespass Support](#)” section on [page 11](#)
- “[Internet Storage Name Service](#)” section on [page 12](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- “Auto-Discovery of SCSI Targets” section on page 12
- “VSAN Membership for iSCSI Interfaces” section on page 12
- “IPS SPAN Source” section on page 12
- “Port Rate Limiting” section on page 12
- “Transceiver and Calibration Information” section on page 13
- “Buffer-to-Buffer Credit Display” section on page 13
- “PortChannel Quiesce” section on page 13
- “Zone Membership” section on page 13
- “Call Home Enhancements” section on page 13
- “FC Domain ID Changes” section on page 14
- “Per VSAN Time Out Values” section on page 15
- “Running Configuration Information” section on page 15
- “Initial Setup Additions” section on page 15
- “Automatic Image Synchronization” section on page 15
- “Standby State” section on page 15
- “Terminal Connection Options” section on page 16
- “Standby Supervisor Module Boot Variables” section on page 16
- “Replacing Modules” section on page 16
- “Deprecated Commands” section on page 16

The Caching Services Module

The Caching Services Module (CSM) provides virtualization services that allow the Cisco MDS 9000 Family switches to reallocate physical resources as virtual resources for increased efficiency. The CSM has two hard drives, two internal batteries for backup in case of power failure, and no external ports. The CSM receives and sends data through the switch backplane. The batteries on the CSM provide adequate power to back up data without external power.

Refer to the documents listed in the “[CSM—Virtualization Documentation](#)” section on page 6.

CSM—Virtualization Documentation

The following documents provide more information on the IBM TotalStorage SAN Volume Controller Storage Software (SVC) and the CSM.

- For CSM information, refer to the *Cisco MDS 9216 Switch Hardware Installation Guide* or the *Cisco MDS 9500 Family Hardware Installation Guide*.
- For SAN-OS CLI configuration information, refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*.
- For SAN-OS CLI commands, refer to the *Cisco MDS 9000 Family Command Reference*.
- For information on IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000, refer to the following IBM documents available on the IBM TotalStorage Support web site: <http://www.ibm.com/storage/support/2062-2300/>

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

- Getting Started—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Configuration Guide—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Supported Hardware List—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Supported Software Levels—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Command Line Interface User's Guide—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Host Attachment Guide—*IBM TotalStorage SAN Volume Controller Storage Software*
- User Guide—*Subsystem Device Driver User's Guide*

Optional 2 RU Shelf Bracket

The Telco and EIA Shelf Bracket Kit is now available (separately orderable); this is a 2 RU Shelf Bracket that allows single-user installation and installation in a Telco rack for the Cisco MDS 9100 Switches, 9216 Switches, and 9506 Directors.

Refer to the *Cisco MDS 9216 Switch* or the *Cisco MDS 9500 Series Hardware Installation Guides*.

Inter-VSAN Routing

VSANs improve Storage Area Network (SAN) scalability, availability, and security by allowing multiple Fibre Channel SANs to share a common physical infrastructure of switches and ISLs. These benefits are derived from the separation of Fibre Channel services in each VSAN and isolation of traffic between VSANs. Data traffic isolation between the VSANs also inherently prevents sharing of resources attached to a VSAN, like robotic tape libraries. Using Inter-VSAN Routing (IVR), resources across VSANs are accessed without compromising other VSAN benefits.

Data traffic is transported between specific initiators and targets on different VSANs without merging VSANs into a single logical fabric with IVR. Fibre Channel control traffic does not flow between VSANs, nor can initiators access any resource across VSANs aside from the designated ones. IVR enables valuable resources like tape libraries are easily shared across VSANs without compromise.

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

Quality of Service

Transaction processing, a low volume, latency sensitive application, requires quick access to requested information. Backup processing requires high bandwidth but is not sensitive to latency. In a network that does not support service differentiation, all traffic is treated identically—they experience similar latency and get similar bandwidths. The Quality of service (QoS) feature in all switches in the Cisco MDS 9000 Family provides four priority levels for service differentiation in Cisco MDS SAN-OS Release 1.3(1).

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

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

FICON

Fibre Connection (FICON) interface capabilities enhances the Cisco MDS 9000 Family by supporting both open systems and mainframe storage network environments. Inclusion of Control Unit Port (CUP) support further enhances the MDS offering by allowing inband management of the switch from FICON processors.

VSANs allow intermixing of FICON and Fibre Channel Protocol (FCP) traffic on the same switch without compromising scalability, availability, manageability and network security. Other FICON capabilities include switch cascading, fabric binding, PortChannels support, FICON native mode, and port swapping.

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

Fabric Binding

The Cisco MDS SAN-OS 1.3(1) fabric binding feature ensures ISLs are only enabled between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis and can only be implemented in FICON VSANs. You can still perform fabric binding configuration in a non-FICON VSAN—these configurations only come into effect after FICON is enabled.

Fabric binding helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. It uses the Exchange Fabric Membership Data (EFMD) protocol in FICON networks to ensure that the list of authorized switches is identical in all switches in the fabric.

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

Registered Link Incident Report

The Registered Link Incident Report (RLIR) function provides a method for a switch port to send a LIR to a registered Nx-port. When a Link Incident Record (LIR) is detected in FICON-enabled switches in the Cisco MDS 9000 Family form a RLIR Extended Link Service (ELS) and sends it to the members in its Established Registration List (ERL).

The Nx-ports interested in receiving the RLIR ELS send Link Incident Record Registration (LIRR) ELS request to the management server on the Switch. The RLIRs are processed on a per-VSAN basis.

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

Licensing

The licensing functionality is available in all switches in the Cisco MDS 9000 Family. This functionality allows you to access specified premium features on the switch after you install the appropriate license for that feature. Licenses are sold, supported, and enforced from Release 1.3(1).

The licensing model defined for the Cisco MDS product line has two options:

- Feature-based licensing: features that are applicable to the entire switch. The cost varies based on a per-switch usage. The following license packages are available:
 - Standard package (free)
 - Enterprise package
 - SAN extension over IP

Send documentation comments to mdsfeedback-doc@cisco.com

- Mainframe
- Fabric Manager Server
- Module-based licensing: features that require additional hardware modules. The cost varies based on a per-module usage. An example is the IPS module using the FCIP feature.

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

New Features for the Cisco Fabric and Device Manager

The new features for the Cisco Fabric and Device Manager for 1.3(1) include:

- A new installation process
- Support for FICON management
- Support for managing Inter-VSAN zones and zonesets
- License installation process
- Fabric Manager Server
- Cisco Traffic Analyzer for Fibre Channel

The Cisco Fabric Manager Server package extends Cisco Fabric Manager by providing historical performance monitoring for network traffic hot-spot analysis, centralized management services and advanced application integration for greater management efficiency in enterprise.

Cisco Traffic Analyzer provides detailed traffic analysis for Fibre Channel using data captured with the Cisco Port Analyzer Adapter. This data is compiled into various graphs and charts which can be viewed with any web browser. Cisco Fabric Manager provides integrated launch capabilities for the Cisco Traffic Analyzer for Fibre Channel.

Refer to the *Cisco MDS 9000 Family Fabric and Device Manager User Guide* for further information.

Common Information Model

The Cisco MDS 9000 Family now provides support for the Common Information Model (CIM) —an object-oriented information model for describing management information in a network/enterprise environment. A CIM-supported client is required to access the CIM server.

The Cisco MDS 9000 Family provides the following CIM server support:

- The fabric profile, zoning control subprofile, enhanced zoning and enhanced zoning control subprofile, switch profile, and blade subprofile are supported.
- A subset of the classes and association classes.
- Support for the XML encoding and CIM operations over HTTP.
- Support for use of HTTPS, which uses Secure Socket Layer (SSL).

Refer to the *Cisco MDS 9000 Family CIM Programming Reference Guide* for further information.

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

Fabric-Device Management Interface

Cisco MDS SAN-OS 1.3(1) provides support for the Fabric-Device Management Interface (FDMI) functionality. FDMI enables management of devices such as Fibre Channel Host Bus Adaptors (HBAs) through inband communication. All FDMI entries are stored in persistent storage and are retrieved when the FDMI process is started.

This addition complements the existing Fibre Channel name server and management server functions—the SAN-OS software can extract the following management information about attached HBAs and host operating systems without installing proprietary host agents:

- Manufacturer, model, and serial number
- Node name and node symbolic name
- Hardware, driver, and firmware versions
- Host operating system (OS) name and version number

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

FC-SP DHCHAP

Fibre Channel Security Protocol (FC-SP) capabilities in Cisco MDS SAN-OS release 1.3(1) provide switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol implemented in Cisco MDS SAN-OS release 1.3(1) to provide authentication between Cisco MDS switches and other devices. It consists of the CHAP protocol combined with the Diffie-Hellman exchange. When you enable FC-SP, DHCHAP is also automatically enabled.

DHCHAP negotiates hash algorithms and DH groups before performing authentication. DHCHAP supports both MD-5 and SHA-1 algorithm-based authentication.

DHCHAP authentication in each direction requires a shared secret password between the initiating device and the receiving device.

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

TACACS+ Authentication

Cisco MDS switches use the Terminal Access Controller Access Control System plus (TACACS+) protocol to communicate with remote AAA servers. You can configure multiple TACACS+ server groups, set timeout values, set the TACACS+ Server address, set the secret key, set the timeout value, define custom attributes, and display TACACS+ server details.

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

RADIUS Enhancements

Cisco MDS switches use the Remote Access Dial-In User Service (RADIUS) protocol to communicate with remote AAA servers and configure multiple RADIUS server groups.

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

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

AAA Server Groups

You can specify remote AAA servers for authentication, authorization and accounting using server groups. You can create a server group using the **aaa group server** command. If required, you can specify multiple server groups. If the MDS switch encounters errors from the server(s) in the first group, it tries the servers in next server group.

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

FCIP Write Accelerator

The FCIP Write Acceleration feature in Cisco MDS SAN-OS release 1.3(1) enables you to significantly improve application performance when storage traffic is routed over wide area networks using FCIP. When FCIP Write Acceleration is enabled, WAN throughput is maximized by minimizing the impact of WAN latency for the command to transfer ready acknowledgement.

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

FCIP Compression

FCIP compression in the Cisco SAN-OS increases the effective WAN bandwidth without costly infrastructure upgrades. By integrating data compression in the IP Storage Services module, more efficient FCIP-based business continuity and disaster recovery solutions can be implemented, without adding and managing a separate device.

Each Gigabit Ethernet port on the IP Storage Services module has its own compression engine. The Lempel-Zif-Stac (LZS) algorithm used for compression typically achieves a 2:1 compression ratio over a wide variety of data sources, delivering a data rate of up to 100 Mbps compressed (up to 200 Mbps uncompressed) per Gigabit Ethernet port on IP Storage Services modules.

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

Proxy Initiator

By default, each iSCSI initiator appears as one Fibre Channel initiator in transparent mode in the Fibre Channel fabric. For some storage arrays, this appearance requires the initiator's pWWN to be manually configured for access control purposes. This process can be quite cumbersome. The Proxy initiator feature allows all iSCSI initiators to connect through one IPS port making it appear as one Fibre Channel port per VSAN. It simplifies the task of configuring the pWWN for each new initiator on the storage array, and Fibre Channel access control such as zoning.

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

Trespass Support

In addition to the high availability of statically imported iSCSI targets, the trespass feature is available, effective Release 1.3(1), to enable the export of Logical Units (LUs), on an active port failure, from the active to the passive port of a statically imported iSCSI target. When the active port fails, the passive port becomes active, and if the trespass feature is enabled, the MDS issues a trespass command to the target to export the LUs on the new active port.

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

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

Internet Storage Name Service

Effective Release 1.3(1), the Internet Storage Name Service (iSNS) client feature is available in all switches in the Cisco MDS 9000 Family with IPS modules installed.

iSNS services allow your existing TCP/IP networks to function more effectively as storage area networks by automating the discovery and management of iSCSI devices. To facilitate these functions, the iSNS client functionality registers iSCSI portals and all targets accessible through a particular interface.

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

Auto-Discovery of SCSI Targets

The **show scsi-target auto-poll** command displays automatically discovered SCSI targets which come online—for example a CSM or an IPS module that inserted in a chassis.

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

VSAN Membership for iSCSI Interfaces

You can configure an iSCSI host to be a member of one or more VSANs. The IPS module creates one Fibre Channel virtual N port in each VSAN to which the host belongs.

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

IPS SPAN Source

Effective Cisco MDS SAN-OS Release 1.3(1) Switched Port Analyzer (SPAN) capabilities are also available on the IP Storage Services (IPS) module. The SPAN feature is only implemented on the FCIP and iSCSI virtual Fibre Channel port interfaces, not the physical Gigabit Ethernet ports. You can SPAN ingress, egress or traffic in both directions for all eight iSCSI and 24 FCIP interfaces that are available in the IPS module.

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

Port Rate Limiting

A port rate limiting feature is available in Cisco MDS SAN-OS release 1.3(1) for switches in the Cisco MDS 9100 Series. This feature helps control the bandwidth for individual Fibre Channel ports. Port rate limiting is also referred to as ingress rate limiting because it controls ingress traffic into a Fibre Channel port. Port rate limiting works on all host-optimized Fibre Channel ports.

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

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

Transceiver and Calibration Information

The **show interface** *interface-type slot/port* **transceiver** command displays real-time diagnostics information for transceivers, including the temperature, voltage, current, tx/rx-power. It also shows the hi/lo alarm and warning thresholds. You can also display transceiver information for a specified fibre channel interface, as well as the calibrations used for computing the diagnostics information—for example, if a SFP is internally calibrated. This command can only be issued on a switch in the Cisco MDS 9100 Series if the FCOT is present.

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

Buffer-to-Buffer Credit Display

The **show interface** command displays the current receive and transmit Buffer-to-Buffer Credit (BB_credit) along with other pertinent interface information for this interface. The BB_credit values are useful to verify situations when the data traffic is slow.

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

PortChannel Quiesce

Generally a **shutdown** command issued on an interface through which traffic is flowing disables the interface with possible frame drop. You can avoid this frame drop, by using the **quiesce** command to gracefully shutdown an interface without dropping any frames. This command can only be issued on an ISL within a PortChannel—at both ends of the link. This command prevents frame loss for a planned link shutdown or removal.

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

Zone Membership

Effective Release 1.3(1) zone membership criteria is also based on the following:

- Interface and domain ID—Specifies the interface of a switch identified by the domain ID.
- Domain ID and port number—Specifies the domain ID of an MDS domain and additionally specifies a port belonging to a non-Cisco switch.
- IP address—Specifies the iSCSI host IP address (and an optional subnet mask) of an attached device.

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

Call Home Enhancements

You can define a Call Home destination profile. The format options for a user-defined destination profile are **full-txt**, **short-txt**, or **XML** (default).

The **alert-group** option allows you to select predefined types of Call Home alert notifications for destination profiles (predefined and user-defined). Destination profiles can be associated with multiple alert groups.

Send documentation comments to mdsfeedback-doc@cisco.com

The **message-level** option allows you to filter messages based on their level of urgency. Each destination profile (predefined and user-defined) is associated with a Call Home message level threshold. Any message with a value lower than the urgency threshold will not be sent. The urgency level ranges from 0 (lowest level of urgency) to 9 (highest level of urgency), and the default is 0 (all messages will be sent).

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

FC Domain ID Changes

SAN-OS 1.3.1 provides an option to define the default behavior for enabling persistent FC IDs. Persistent FC IDs are disabled by default. You can enable this option globally or for each VSAN.

It is no longer necessary to assign a static Domain ID to a MDS before enabling the persistent FC ID feature.

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

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

Per VSAN Time Out Values

You can issue the **ftimer** command for a specified VSAN to configure different Time Out Values (TOV) for VSANs with special links like FC or IP tunnels.

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

Running Configuration Information

You can gather specific information on the entire switch configuration by issuing the relevant **show** commands. Configurations are displayed based on a specified feature, interface, module, or VSAN.

- The **show running diff** command displays the difference between the running and startup configuration.
- The **show running interface** command displays the configuration for a specified interface.
- The **show running vsan** command displays the configuration per VSAN.

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

Initial Setup Additions

You have the option to enable a full zoneset distribution and to enable FC ID persistence for the entire fabric while configuring the initial setup.

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

Automatic Image Synchronization

The running image is automatically synchronized in the standby supervisor module by the active supervisor module. The boot variables are synchronized during this process. The standby supervisor module, automatically synchronizes its image with the running image on the active supervisor module.

Effective Cisco MDS SAN-OS release 1.3(1) the automatic synchronization feature (previously known as the **auto-sync** command) is enabled by default in all switches in the Cisco MDS 9000 Family. This command is no longer configurable.

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

Standby State

The internal standby state indicates that a switchover is possible when the redundancy state or the supervisor state display standby or HA standby. A warm standby is no longer used in the Cisco MDS switches.

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

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

Terminal Connection Options

From the active supervisor module, you can connect to a console terminal, a Telnet terminal, or an SSH terminal.

When you issue an **install all** command from a console terminal connected to the active supervisor and a switchover happens, you can continue to see the rest of the output from the console terminal of the standby supervisor module.

Similarly, you can view the results of the **install all** command issued from the SSH or Telnet terminal that is connected to the active supervisor. Once a switchover happens, you need to log back into the switch and issue the **show install all status** command.

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

Standby Supervisor Module Boot Variables

If the standby supervisor module's boot variable images are not the same version as those running on the active supervisor module, the software forces the standby supervisor module to run the same version as the active supervisor module.

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

Replacing Modules

When you replace any module (supervisor, switching, or services module), ensure that the new module is running the same software version as the rest of the switch. Issuing the **install all** command after replacing any module, ensures the following actions:

- The proper system and kickstart images are copied on the standby bootflash.
- The proper boot variables are set.
- The loader and the BIOS are upgraded to the same version available on the active supervisor module.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for configuration details on replacing all other modules.

Deprecated Commands

The following commands were deprecated:

- **system upgrade-reset** and **system no upgrade-reset** (no longer required)
- **auto-sync** (automatic synchronization is always enabled)
- **show interface fcbbcredit** (replaced by **show interface bbcredit**)
- **show interface fc slot/port fcbbcredit** (replaced by **show interface fc slot/port bbcredit**)

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

Limitations and Restrictions

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

Send documentation comments to mdsfeedback-doc@cisco.com

- [Downgrading to Cisco MDS SAN-OS Release 1.0\(x\), page 17](#)
- [Port Rate Limiting, page 17](#)
- [Transceiver and Calibration Information, page 17](#)
- [Configuring TOVs, page 17](#)
- [Uninstalling Licenses, page 18](#)
- [System Switchover, page 18](#)
- [IVRs, page 18](#)
- [No AAA Authentication, page 18](#)
- [CHAP Authentication, page 18](#)
- [FICON, page 19](#)

Downgrading to Cisco MDS SAN-OS Release 1.0(x)

If IP routing is enabled in Cisco MDS SAN-OS Release 1.0(x), the switch does not use the configured default gateway and cannot be reached from a different subnet.

When downgrading from Release 1.1(x), 1.2(x), or 1.3(x) to Release 1.0(x) and the IP routing option is enabled in any switch in the Cisco MDS 9000 Family, you must disable the IP routing feature before or immediately after the downgrade procedure is complete.

Port Rate Limiting

The port rate limiting feature can only be configured if the following conditions hold true:

- The QoS feature is enabled using the **qos enable** command.
- The command can only be issued in a Cisco MDS 9100 Series switch.

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

Transceiver and Calibration Information

The **show interface interface-type slot/port transceiver** command can only be issued on a switch in the Cisco MDS 9100 Series if the FCOT is present.

Configuring TOVs

Fibre Channel TOVs can not be changed unless all VSANs in the switch are suspended.

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)

Uninstalling Licenses

You can only uninstall a permanent license that is not in use. If you try to delete a permanent license that is currently being used, the software rejects the request and issues an error message. Uninstalling an unused license causes the grace period to come into effect. The grace period is counted from the first use of the feature without a license and is reset when a valid license file is installed. Uninstalling a license requires the related features to first be disabled.

After the final seven days of a grace period, the licensed feature is turned off and your network traffic may be disrupted. The grace period also applies to licensed features in Release 1.2(x). While Release 1.2(x) did not enforce the licenses, any upgrade will enforce license requirements and the 60-day grace period.

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

System Switchover

If the supervisor modules are not in a stable state (online or powered down), a switchover will not be performed.

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

IVRs

Active IVR topologies cannot be deactivated.

Using the **force** option of Inter-VSAN Zone Sets (IVZS) activation may cause traffic disruption, even for devices that are not involved in IVR. For example, if your configuration does not have any active zone sets and the default zone policy is **permit**, then an IVZS activation will fail. However, IVZS activation will go through if the **force** option is used. Since zones are created in the edge VSANs corresponding to each Inter-VSAN Zone (IVZ), traffic may be disrupted in edge VSANs where the default zone policy is permit.

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

No AAA Authentication

You can turn off password verification using the **none** option in the **aaa authentication login** command. If you configure this option, users will be able to login without giving a valid password as long as the user exists locally on the MDS switch.(created using the **username** command). Use this option cautiously. If configured, any user will be able to access the switch at any time.

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

CHAP Authentication

RADIUS and TACACS+ protocols always use MD-5 for CHAP authentication. Using SHA-1 as the hash algorithm may prevent RADIUS and TACACS+ usage—even if these AAA protocols are enabled for DHCHAP authentication.

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)

FICON

When you disable the FICON feature, the FICON configuration file (called the IPL file) is automatically deleted and cannot be recovered.

You cannot deactivate or disable fabric binding in a FICON-enabled VSAN.

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

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)	
	1.2(2a)	1.3(1)
Severity 1		
CSCeb13329	O	R
CSCed10846		O
CSCee18613		O
Severity 2		
CSCec46067	O	R
CSCec62235	O	R
CSCed57251		O
CSCed65607	O	O
CSCed75825	O	O
CSCee01143	O	O
CSCee06496	O	O
CSCee43249	O	O
CSCef83504		O
CSCeg84871	O	O
CSCei25319	O	O
CSCsh27840	O	O
Severity 3		
CSCec31365		O
CSCdz12179	O	O
CSCdz43707	O	O
CSCea45726	O	O
CSCea82028	O	O
CSCeb19588	O	R

Send documentation comments to mdsfeedback-doc@cisco.com

Table 3 *Release Caveats and Caveats Corrected Reference (continued)*

DDTS Number	Software Release (Resolved or Open)	
	1.2(2a)	1.3(1)
CSCeb34865	O	O
CSCeb83984	O	R
CSCec10009	O	O
CSCec79467		O
CSCed13757		O
CSCed14360		O
CSCed14920		O
CSCed32729	O	O
CSCed58155	O	O
CSCed64425	O	O
CSCed94302		O
CSCee89946	O	O
CSCeg61535	O	O
CSCeg66225	O	O
CSCeh21199	O	O
CSCei91676		O
CSCej08751		O
CSCin81760		O
Severity 4		
CSCeh42252	O	O

Resolved Caveats

- [CSCeb13329](#)
Symptom: Under certain configuration scenarios, the VXSVC daemon in the Application Services Module (ASM) may run out of memory.
Workaround: None. Upgrade to Cisco MDS SAN-OS 1.3(1).
- [CSCec46067](#)
Symptom: During relayout or recovery operations, the I/O performance of the ASM was lower than expected.
Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.3(1) or later.
- [CSCec62235](#)
Symptom: HBA ports require a different area ID than storage ports when they are both connected to the same switch. For example, if the storage port FCID is 0x6f0004, the area for this port is 00. In this case, the HBA port's area can be anything other than 00. The HBA port's FC ID must be manually configured to be different from the storage port's FC ID.

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

Workaround: Refer to the *Release 1.2(2a) Cisco MDS 9000 Family Configuration Guide* for a detailed procedure on assigning different area FC IDs.

- CSCeb19588

Symptom: Sometimes, the **zone merge import** command results in isolation.

Workaround: Reissue the command to resolve the isolation problem.

- CSCeb83984

Symptom: When downgrading a Cisco MDS 9000 Family switch to an older release version which does not contain the LUN zoning feature, for example, Release 1.1(x), the configuration is not erased completely.

Workaround: Delete the LUN zoning configuration before downgrading the switch.

Open Caveats

- CSCed10846

Symptom: Module-specific information will not be saved properly in the startup configuration if saved with a fresh boot (boot with no saved config) of 1.3(1) and will be lost when the switch is reload. This does not happen during an upgrade from Cisco MDS SAN-OS Release 1.2(x) to 1.3(1) to 1.3(2a).

Workaround: Do not save startup configuration with a fresh boot of 1.3(1).

- CSCee18613

Symptom: The name server loses route entries (well-known address routes) when a new module is inserted or if an existing module is reset in a Cisco MDS 9000 Family switch that has been nondisruptively upgraded to SAN-OS 1.3(2a) or 1.3(3) from a SAN OS release 1.0(x), or 1.1(x), or 1.2(x). This results in the host is unable to communicate with that module.

Workaround:

- This bug is fixed in Release 1.3(3c) and all subsequent releases.
- If you received the Cisco MDS Switch with a factory-installed SAN-OS Release 1.3(x), you will not be affected by this bug.
- If you are currently running SAN-OS Releases 1.0(x), 1.1(x), or 1.2(x) and planning to upgrade to Releases 1.3(2a) or 1.3(3), be sure to schedule a switch reload after the SAN-OS upgrade.

- 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.

- 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

Send documentation comments to mdsfeedback-doc@cisco.com

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.
- Configuring the new module.
- 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).

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCec31365

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

Workaround: None.

- CSCdz12179

Symptom: When the Fabric Manager or Device Manager communicates with the Cisco MDS switch through Virtual Private Network (VPN) or any Network Address Translation (NAT) scheme, a generic error message occurs while adding duplicate zone members from a VPN connection.

Workaround: None. If an error occurs while running through VPN/NAT, all errors will show up as generic errors without a detailed message describing the error.

- CSCdz43707

Symptom: The Fabric Manager or Device Manager reports an error for all operations if the switch is multi-homed (both IPFC-based in-band management and the out-of-band management interface are up) and the Fabric or Device Manager was started using the IPFC address. Typically, you will see a `notInTime window` error in the Device Manager and all SNMP set operations fail.

Workaround: If the switch is multi-homed, then start the Fabric or Device Manager on the switch using the out-of-band management interface IP address.

- CSCea45726

Send documentation comments to mdsfeedback-doc@cisco.com

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.

- CSCeb34865

Symptom: The following error message is issued when you try configuring switch drop latency:
`changing this parameter is not allowed could not update the value`

Workaround: None. Switch drop latency is not configurable in this release of the software.

- 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.

- CSCec79467

Symptom: When running with McData's 5.0 firmware, the fabric may stall after the E-port is up.

Workaround: None.

- CSCed13757

Symptom: When the FCIP write acceleration feature is enabled, IPFC frames and related Fibre Channel exchanges may not be handled correctly—the IPFC traffic generated using a ping function did not follow the specified exchange management assumptions and norms.

Workaround: None.

- 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.

- 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`.

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

- 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.

- CSCed32729

Symptom: When altering an Fx-port state using SNMP, the following error is reported:

```
snmpset: Agent reported error with variable #1.
.iso.org.dod.internet.mgmt.mib-2.75.1.2.2.1.1.22.0:  SNMP: A general
failure occurred on the agent.
```

Workaround: None.

- 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
```

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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
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)
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: None. Enable the license features again.

- 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.

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 Release 1.3(1)*
- *Cisco MDS 9100 Series Quick Start Guide*
- *Cisco MDS 9500 Series and Cisco MDS 9216 Switch Quick Start Guide*
- *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 and Device Manager User Guide*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family System Messages Guide*
- *Cisco MDS 9000 Family MIB Reference Guide*
- *Cisco MDS 9000 Family CIM Programming Reference Guide*

For information on VERITAS Storage Foundation™ for Networks 1.0, Cisco, refer to the following VERITAS documents available at <http://support.veritas.com/>

- *VERITAS Storage Foundation for Networks Overview*
- *VERITAS Storage Foundation for Networks Installation and Configuration Guide*
- *VERITAS Storage Foundation for Networks Obtaining and Installing Licenses*
- *VERITAS Storage Foundation for Networks GUI Administrator's Guide*
- *VERITAS Storage Foundation for Networks CLI Administrator's Guide*
- *VERITAS Storage Foundation for Networks README*

For information on IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000, refer to the following IBM documents available on the IBM TotalStorage Support web site: <http://www.ibm.com/storage/support/2062-2300/>

- *Getting Started—IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*

Send documentation comments to mdsfeedback-doc@cisco.com

- Configuration Guide—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Supported Hardware List—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Supported Software Levels—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Command Line Interface User's Guide—*IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000*
- Host Attachment Guide—*IBM TotalStorage SAN Volume Controller Storage Software*
- User Guide—*Subsystem Device Driver User's Guide*

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/>

Send documentation comments to mdsfeedback-doc@cisco.com

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/>

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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>



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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

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>

Send documentation comments to mdsfeedback-doc@cisco.com

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

