Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.0(1b)

Release Date: October 22, 2004

Text Part Number: OL-6249-01 Rev. F1

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 39.

Note Releases 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 History Change

Revision	Date	Description
A0	10/22/2004	Release notes created
B0	11/05/2004	Table 2 caption revised Table 3 correctly referenced in the Caveats section
C0	11/09/2004	Added SSE license information
D0	11/17/2004	Added DDTS CSCeg23889, image upgrade references, and FC ID information
E0	11/30/2004	Added Fabric Manager/Device Manager Support on Windows2003 information
F0	12/15/2004	Added DDTS CSCeg53094
G0	12/22/2004	Added DDTS CSCeg59198, CSCeg61535, and CSCeg58996
H0	01/14/2005	Added DDTS CSCef74578, CSCef82882, CSCef94903, CSCeg05450, CSCeg09210, CSCeg37598, CSCeg44018, CSCeg46989, CSCeg56197.
I0	02/17/2005	Added DDTS CSCef83504

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

Table 1 On-Line History Change (continued)

Revision	Date	Description
J0	02/28/2005	Added DDTS CSCeg85146 and CSCin81851
K0	03/15/2005	Added DDTS CSCeh21199, CSCef56229
L0	03/24/2005	Added DDTS CSCed20053, CSCef65409, CSCef70000, CSCeg13762, CSCeg17593, CSCeg18886, CSCeg20292, CSCeg30690, CSCeg33732CSCin81760. Changed severity of DDTS CSCeg44018.
M0	04/12/2005	Added DDTS CSCeg07325, CSCeh44216, CSCeh49026, CSCeh51924
N0	04/13/2005	Added DDTS CSCeg81089
O0	5/3/2005	Added DDTS CSCeh65824
P0	5/19/2005	Removed DDTS CSCeh44216
Q0	5/24/2005	Added DDTS CSCeg66225 and CSCeh42252
R0	5/31/2005	Added DDTS CSCeh96928
S0	06/01/2005	Added DDTS CSCeg24199
T0	06/23/2005	Added DDTS CSCei25319
U0	07/29/2005	Added DDTS CSCed57251, CSCeh61610, CSCeh64080, CSCec31365, CSCeg20932, CSCeg53114, CSCeg66225, CSCeh19639, CSCeh52280, CSCeh56143, CSCeh82490, CSCeh83514, and CSCeh87985
V0	08/05/2005	Added DDTS CSCeh41099
W0	08/22/2005	Removed DDTS CSCeh61610
X0	08/23/2005	Added DDTS CSCeh61610
Y0	10/14/2005	Modified DDTS CSCeg07325
Z0	12/07/2005	Added DDTS CSCsc31424
A1	12/30/2005	Added DDTS CSCei91968
B1	05/02/2006	Added DDTS CSCeg33121, CSCei67982, CSCei91676, and CSCsc33788
C1	06/06/2006	Removed DDTS CSCed16845
D1	9/05/2006	Added DDTS CSCsd78967
E1	9/13/2006	Added DDTS CSCsf21970
F1	02/23/2007	Added DDTS CSCsg03171 and CSCsh27840.

Contents

This document includes the following sections:

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.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 2.0(1b) and includes the following topics:

Components Supported

Table 2 lists the software and hardware components supported by the Cisco MDS 9000 Family.

Note To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S1K9-2.0.1	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-2.0.1	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-2.0.1	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only

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

Component	Part Number	Description	Applicable Product
License	M9500SSE1K9	Storage services enabler package	MDS 9500 series with ASM
	M9500SSE1K9	Storage services enabler package	MDS 9200 series with ASM
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 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately.	MDS 9216i only
	DS-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-Gbps/1-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 2-Gbps/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).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	

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

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	2-Gbps/1-Gbps Fibre Channel — short wave SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW	2-Gbps/1-Gbps Fibre Channel — long wave SFP.	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 2-Gbps/1-Gbps Fibre Channel—short wave SFP.	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 2-Gbps/1-Gbps Fibre Channel — long wave SFP.	
CWDM[2]	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 2-Gbps/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	300-W[3] AC power supply.	MDS 9100 Series only
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2	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 wavelength division multiplexing
3. W = Watt

Determining the Software Version

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

To determine the version of the Cisco MDS 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 MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, view the Switches tab in the information pane, locate the switch, using the IP address, logical name, or WWN, and check its version in the Release column.

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 Cisco MDS SAN-OS Release 2.0(1b) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of SAN-OS, upgrade to Release 1.3(x) and then Release 2.0(1b).

When downgrading from Cisco MDS SAN-OS Release 2.0(1b) to release 1.3(x), you might need to disable new features in release 2.0(1b) for a nondisruptive downgrade. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade, enables the compatibility check which will indicate that the downgrade will be disruptive and the reason will be "current running-config is not supported by new image".

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
      2       yes      disruptive         reset  Current running-config is not supported
by new image
      3       yes      disruptive         reset  Current running-config is not supported
by new image
      5       yes      disruptive         reset  Current running-config is not supported
by new image
      6       yes      disruptive         reset  Current running-config is not supported
by new image
```

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:1.3(x)_filename** command determines which additional features need to be disabled.

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

New Features in Cisco MDS SAN-OS Release 2.0(1b)

Cisco MDS SAN-OS Release 2.0(1b) is a major release for switches in the Cisco MDS 9000 Family. See the "Caveats" section on page 25 for details on closed and outstanding caveats and limitations.

Note These Release Notes are specific to this release. For the Cisco MDS SAN-OS Release 2.x documentation, set, see the "Related Documentation" section on page 39.

The following new features are introduced in Release 2.0(1b):

Cisco MDS 9216i Multiprotocol Fabric Switch

Cisco MDS 9216i multiprotocol fabric switches contain one fixed integrated supervisor module with 14 Fibre Channel ports, 2 IP ports that can support FCIP and iSCSI protocols simultaneously, and an expansion slot that can support up to 32 additional ports (for a total of 48 ports).

The Cisco MDS 9216i switch shares a consistent software architecture with the Cisco MDS 9500 Series in a semi-modular chassis and consists of the following major hardware components:

- The chassis has two slots, one of which is reserved for the integrated supervisor module. The supervisor module provides supervisor functions and has 14 standard, Fibre Channel ports and two multiprotocol ports that can support FCIP and iSCSI protocols simultaneously.
- One hot-pluggable switching or services module that provides Fibre Channel or Gigabit Ethernet services.
- The backplane has direct plug-in connectivity to one switching or services module (any type).
- The hot-swappable fan module has four fans managing the airflow and cooling for the entire switch.
- These fabric switches also have the following features:
  - Two redundant, hot-swappable power supplies have AC connections, each of which can supply power to a fully loaded chassis.
  - The 1-Gbps or 2-Gbps autosensing Fibre Channel ports support Inter-Switch Links (E ports), extended Inter-Switch Links (TE ports), loops (FL and TL ports), and fabric (F ports) connectivity. Besides Telnet access, a 10/100BASE-T Ethernet port provides switch access and an RS-232 (EIA/TIA-232) serial port allows switch configuration.
  - Hot-swappable, small form-factor pluggable (SFP) ports can be configured with either short or long wavelength SFPs for connectivity up to 500 m and 10 km, respectively. The ports can also be configured with the extended wavelength SFPs for connectivity up to 100 km.
  - The Cisco MDS 9200 Series support the IP Storage Services (IPS) module and the 14/2-port Multiprotocol Services (MPS-14/2) module. Both modules are configurable for both FCIP and iSCSI operation on a port-by-port basis. Ports configured for FCIP operation can be further configured to support up to three virtual ISL connections.

Refer to the *Cisco MDS 9200 Series Hardware Installation Guide*.

Cisco MDS 9216A Multilayer Fabric Switch

Cisco MDS 9216A multilayer fabric switches contain one fixed integrated supervisor module with 16 Fibre Channel ports and an expansion slot that can support up to 32 additional ports (for a total of 48 ports).

The Cisco MDS 9216 Switch and the Cisco MDS 9216A Switch share a consistent software architecture with the Cisco MDS 9500 Series in a semi-modular chassis and consists of the following major hardware components:

- The chassis has two slots, one of which is reserved for the integrated supervisor module. The supervisor module provides supervisor functions and has 16 standard, Fibre Channel ports.
- One hot-pluggable switching or services module that provides Fibre Channel or Gigabit Ethernet services.
- The backplane has direct plug-in connectivity to one switching or services module (any type).
- The hot-swappable fan module has four fans managing the airflow and cooling for the entire switch.

- These fabric switches also have the following features:
  - Two redundant, hot-swappable power supplies have AC connections, each of which can supply power to a fully loaded chassis.
  - The 1-Gbps or 2-Gbps autosensing Fibre Channel ports support Inter-Switch Links (E ports), extended Inter-Switch Links (TE ports), loops (FL and TL ports), and fabric (F ports) connectivity. Besides Telnet access, a 10/100BASE-T Ethernet port provides switch access and an RS-232 (EIA/TIA-232) serial port allows switch configuration.
  - Hot-swappable, small form-factor pluggable (SFP) ports can be configured with either short or long wavelength SFPs for connectivity up to 500 m and 10 km, respectively. The ports can also be configured with the extended wavelength SFPs for connectivity up to 100 km.
  - The Cisco MDS 9200 Series support the IP Storage Services (IPS) module and the 14/2-port Multiprotocol Services (MPS-14/2) module. Both modules are configurable for both FCIP and iSCSI operation on a port-by-port basis. Ports configured for FCIP operation can be further configured to support up to three virtual ISL connections.

Refer to the *Cisco MDS 9200 Series Hardware Installation Guide*.

14/2-Port Multiprotocol Services Module

The 14/2-port Multiprotocol Services (MPS-14/2) module allows you to use FCIP and iSCSI features. It integrates seamlessly into the Cisco MDS 9000 Family, and supports the full range of features available on other switching modules, including VSANs, security, and traffic management. The MPS-14/2 module has 14 Fibre Channel ports and two Gigabit Ethernet ports.

Refer to the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.

Graceful Shutdown

As of Release 2.0(1b), the Cisco MDS SAN-OS software implicitly performs a graceful shutdown in response to either of the following actions:

- If you shutdown an interface operating in the E port mode
- If a Cisco MDS SAN-OS software application executes a port shutdown as part of its function

A graceful shutdown ensures that no frames are lost when the interface is shutting down. When a shutdown is triggered either by you or the Cisco MDS SAN-OS software, the switches connected to the shutdown link coordinate with each other to ensure that all frames in the ports are safely sent through the link before shutting down. This enhancement reduces the chance of frame loss.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Cisco Fabric Services

The Cisco MDS SAN-OS software uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database distribution and to foster device flexibility. It simplifies SAN provisioning by automatically distributing configuration information to all switches in a fabric. The following Cisco MDS SAN-OS features use the CFS infrastructure:

- TACACS and RADIUS
- Dynamic Port VSAN Membership
- Distributed Device Alias Services
- iSNS
- Call Home
- Port security
- Syslog
- User and administrator roles
- IVR topology
- Fctimer
- NTP

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Dynamic VSANs

Port VSAN membership on the switch is assigned on a port-by-port basis. By default each port belongs to the default VSAN.

As of Cisco MDS SAN-OS Release 2.0(1b), you can dynamically assign VSAN membership to ports by assigning VSANs based on the device WWN. This method is referred to as the Dynamic Port VSAN Membership (DPVM) feature. DPVM offers flexibility and eliminates the need to reconfigure the VSAN to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches. It retains the configured VSAN regardless of where a device is connected or moved.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Enhanced Zoning

As of Cisco MDS SAN-OS Release 2.0(1b), the zoning feature is enhanced to be compliant with FC-GS-4 and FC-SW-3. Both standards support the basic zoning and the enhanced zoning functionalities.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Zone-Based Traffic Priority

As of Cisco SAN-OS Release 2.0(1b), the zoning feature provides an additional segregation mechanism to prioritize select zones in a fabric and set up access control between devices. Using this feature, you can configure the Quality of Service (QoS) priority as a zone attribute. You can assign the QoS traffic priority attribute to be high, medium, or low. By default, zones with no specified priority are implicitly assigned a low priority. Zone-based QoS can only be implemented in Cisco MDS 9000 Family switches running Cisco MDS SAN-OS Release 2.0(1b) or later.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Device Alias Distribution

As of Cisco SAN-OS Release 2.0(1b), all switches in the Cisco MDS 9000 Family offer a new alias distribution feature called Distributed Device Alias Services (device alias). In Release 1.3 and earlier, aliases were distributed on a per VSAN basis. Using this new, enhanced service, you now have the option to distribute device alias names on a fabric-wide basis.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Switch Security

Management security in any switch in the Cisco MDS 9000 Family provides security to all management access methods including the command-line interface (CLI) or Simple Network Management Protocol (SNMP). CLI security options also apply to the Cisco MDS Fabric Manager and Device Manager.

- As of Cisco SAN-OS Release 2.0(1b), both the CLI security database and the SNMP user database are synchronized and continue to use the same password that was previously configured.

  Prior to Release 2.0(1b), if a user was previously configured in one database and not the other, the user can continue using that account.

  Prior to upgrading to Release 2.0(1b), if the user was present in the SNMP database and the CLI database, then the set of roles assigned to this user in Release 2.0(1b) will include the union of both sets of roles.
- If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. Passwords are case-sensitive. As of Release 2.0(1b), admin is not the default password for any switch in the Cisco MDS 9000 Family. You must explicitly configure a strong password.
- You can have separate AAA configurations for Telnet or SSH login, console login, iSCSI authentication, FC-SP authentication, or accounting. Server group, local, and none are the three options for any service in an AAA configuration. Each option is tried in the order specified. If all methods fail, local is tried—even if it is not specified as one of the options.
- As of Cisco SAN-OS Release 2.0(1b), the **priv** option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The **priv** option along with **aes-128** token indicates that this privacy password is for generating 128-bit AES key.The AES priv password can have a minimum of 8 characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters. If you use the localized key, you can specify a maximum of 130 characters.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Network Security

The IP Security (IPsec) Protocol is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. It is developed by the Internet Engineering Task Force (IETF). IPsec provides security services at the IP layer, including protecting one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPsec uses the Internet Key Exchange (IKE) protocol to handle protocol and algorithm negotiation and to generate the encryption and authentication keys to be used by IPsec. While IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

PortChannel Protocol

The PortChannel Protocol expands the PortChannel functional model in Cisco MDS switches. Each switch uses the information received from the peer ports along with its local configuration and operational values to decide if it should be part of a PortChannel.

The PortChannel feature now includes a new mode (ACTIVE) and a new protocol (autocreation).

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

ACTIVE Mode

You can configure each PortChannel with a channel group mode parameter to determine the PortChannel protocol behavior for all member ports in this channel group. In the ACTIVE mode, the member ports initiate the PortChannel protocol negotiation with peer port(s) regardless of the channel group mode of the peer port.

The default ON mode is backward compatible with the existing implementation of PortChannels in releases prior to Release 2.0(1b), where the channel group mode is implicitly assumed to be ON. In Cisco MDS SAN-OS Release 1.3 and earlier, the only available PortChannel mode was ON.

Autocreation

As of Cisco SAN-OS Release 2.0(1b), a protocol to exchange PortChannel configurations is available in all Cisco MDS switches. The autocreation mode enables ISLs with compatible parameters to automatically form channel groups without manual intervention.

Port Tracking

The Port Tracking feature is unique to the Cisco MDS 9000 Family of switches. This feature uses information about the operational state of the link to initiate a failure in the link that connects the edge device. This process of converting the indirect failure to a direct failure triggers a faster recovery process. When enabled, the port tracking feature brings down the configured links based on the failed link and forces the traffic to be redirected to another redundant link.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Call Home

As of Cisco SAN-OS Release 2.0(1b), the Call Home feature provides message throttling capabilities, periodic inventory messages, port syslog messages, and RMON alert messages.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

SAN Extension Tuner

The SAN extension tuner (SET) feature is unique to the Cisco MDS 9000 Family of switches. This feature helps you optimize FCIP performance by generating SCSI I/O commands and directing such traffic to a specific virtual target. You can specify the size of the test I/O transfers and how many concurrent I/Os to generate while testing. The SET reports the resulting I/Os per second (IOPS) and I/O latency, which helps you determine the number of concurrent I/Os needed to maximize FCIP throughput.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Command Scheduler

The Cisco MDS command scheduler feature helps you schedule configuration and maintenance jobs in any switch in the Cisco MDS 9000 Family. This feature is available in the Cisco SAN-OS Release 2.0(1b) software. You can use this feature to schedule jobs on a one-time basis or periodically.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Initial Setup Changes

The questions in the initial set up routine and the order in which they appear is enhanced to reflect the various changes in the Cisco SAN-OS Release 2.0(1b) software.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Extended BB_Credits

The BB_credits feature allows you to configure up to 255 receive buffers. This number is insufficient for long haul links. To facilitate BB_credits for long haul links, the extended BB_credits flow control mechanism allows you to configure up to 3,500 receive BB_credits on a Fibre Channel port. The extended BB_credit configuration takes precedence over the receive BB_credit and performance buffer configurations.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Link Initialization WWN Usage

Exchange Link Protocol (ELP) and Exchange Fabric Protocol (EFP) use WWNs during link initialization. The usage details differ based on the Cisco SAN-OS software release:

- In Cisco SAN-OS Release 1.0 and 1.1, both ELPs and EFPs use the VSAN WWN during link initialization.
- In Cisco SAN-OS Releases 1.2 and 1.3, two different WWNs are used during the link initialization process:
  - ELPs use the switch WWN.
  - EFPs use the VSAN WWN.
- In Cisco SAN-OS Release 2.0(1b), both ELPs and EFPs use the VSAN WWN by default during link initialization. However, the ELP usage changes based on the peer switch's usage:
  - If the peer switch ELP uses the switch WWN, then the local switch also uses the switch WWN.
  - If the peer switch ELP uses the VSAN WWN, then the local switch also uses the VSAN WWN.

This link initialization change between Cisco SAN-OS releases is implicit and does not require any configuration.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Multicast Compliance

Prior to Cisco SAN-OS Release 2.0(1b), the principal switch to compute the multicast tree. Now, to interoperate with other vendor switches (following FC-SW3 guidelines), the Cisco SAN-OS software uses the lowest domain switch as the root to compute the multicast tree in interop mode.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

FC ID Enhancements

The FC ID feature is enhanced as described in this section.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Persistence by Default

To preserve the FC IDs in your configuration, verify that the persistent Fibre Channel ID (FC ID) feature is enable before rebooting. As of SAN-OS Release 2.0(1b), this feature is enabled by default. In earlier releases, the default is disabled. For more information on persistent FC ID, see the Persistent FC IDs section in the *Cisco MDS 9000 Family Configuration Guide*.

Allocation for HBAs

To conserve the number of FC IDs used, Cisco MDS 9000 Family switches use a special FC ID allocation scheme.

In Cisco SAN-OS Release 1.3 and earlier, a full area is allocated to host bus adapters (HBAs). This allocation isolates them to an area and they are listed with their pWWN during a fabric login. The allocated FC IDs are cached persistently and are still available in Cisco SAN-OS Release 2.0(1b).

To allow further scalability for switches with numerous ports, the Cisco SAN-OS Release 2.0(1b) software maintains a list of HBAs, identified by their company IDs (also known as Organizational Unit Identifier, or OUI), that use the pWWN during a fabric log in. A full area is allocated to N ports with company IDs that are listed and for the others, a single FC ID is allocated. Irrespective of the kind (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

Changed Term from FCOT to SFP

As of Cisco SAN-OS Release 2.0(1b), the term FCOT (Fibre Channel optical transmitter), is replaced by the term SFP (small form-factor pluggable), in the Cisco SAN-OS software and in the documentation.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

IP-ACL Enhancements

In Cisco SAN-OS Release 1.3 and earlier, you could only apply IP-ACLs to VSAN interfaces and the management interface. As of Cisco SAN-OS Release 2.0(1b), you can also apply IP-ACLs to Gigabit Ethernet interfaces (IPS modules) and Ethernet PortChannel interfaces.

If IP-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Do not apply IP-ACLs to only one member of a PortChannel group. Apply IP-ACLs to the entire channel group.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Storing the Last Core to Flash

As of Cisco SAN-OS Release 2.0(1b), the last core dump (service core) is automatically saved to the Flash in the /mnt/pss/ partition before the switchover or reboot occurs. Three minutes after the supervisor module reboots, the saved last core is restored from the Flash partition (/mnt/pss) back to its original RAM location. This restoration is a background process and is not visible to the user.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

File System Enhancements

As of Cisco SAN-OS Release 2.0(1b), you can use the **Tab** key to complete schemes, servers, and file names available in the file system.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

RMON Configuration

As of Cisco SAN-OS Release 2.0(1b), you can configure RMON alarms and events by using the CLI.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

IP Storage

This section includes the following subsections:

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

FCIP Tape Acceleration

Tapes are storage devices that store and retrieve user data sequentially. Applications that access tape drives normally have only one SCSI WRITE operation outstanding to it. This single command process limits the benefit of the write acceleration feature when using an FCIP tunnel over a long-distance WAN link. It impacts backup and archive performance because each SCSI WRITE operation does not complete until the host receives a good status response from the tape drive.

The FCIP tape acceleration feature is introduced in Cisco SAN-OS Release 2.0(1b) to improve tape backup and archive operations by allowing faster data streaming from the host to the tape over the WAN link.

FCIP Compression Enhancement

The FCIP compression feature is enhanced to support new compression modes

- **mode 1 i**s recommended for link with bandwidth higher than 25 Mbps.
- **mode 2** is recommended for link with bandwidth lower than 25 Mbps but higher than 10 Mbps.
- **mode 3** is recommended for link with bandwidth lower than 10 Mbps.

These three modes replace the **high-throughput** and **high-comp-ratio** modes available in Cisco SAN-OS Release 1.3.

When you upgrade from Cisco SAN-OS Release 1.3, the **high-throughput** configuration becomes **mode 1** and the **high-comp-ratio** configuration becomes **mode 3**.

When you downgrade from Cisco SAN-OS Release 2.0(1b) to Cisco SAN-OS Release 1.3 release, all modes (**mode 1**, **mode 2**, and **mode 3**) in Cisco SAN-OS Release 2.0(1b) become **high-throughput** mode in Cisco SAN-OS Release 1.3.

iSNS Server

The iSNS server allows existing TCP/IP networks to function more effectively as storage area networks by automating the discovery, management, and configuration of iSCSI devices. It also provides device registration, state change notification, and remote domain discovery services.

Mutual CHAP Authentication

The IPS module supports a mechanism for the iSCSI initiator to authenticate the switch using the switch user name and password during the iSCSI CHAP authentication login.

Other IP Storage Changes

The following settings are enhanced in Cisco SAN-OS Release 2.0(1b):

- Forwarding mode—The store-and-forward mode is the default iSCSI forwarding mode.
- Time stamp control—The default value for packet acceptance is 2000 microseconds. In Cisco SAN-OS Release 1.3 and earlier, the burst size was 1000 microseconds.
- Maximum delay jitter—The default value for FCIP interface is 1000 microseconds. In Cisco SAN-OS Release 1.3, the burst size was 100 microseconds.
- Monitoring window congestion—The default burst size is 50 KB. In Cisco SAN-OS Release 1.3 and earlier, the burst size was 10 KB.
- Write acceleration—FCIP write acceleration works even if the FCIP port is part of a PortChannel. In releases prior to SAN-OS 2.0(1b) FCIP write acceleration does not work if the FCIP port is part of a PortChannel.

New CLI Commands

Several new CLI commands support the new features in this software release. Other commands introduced or significantly enhanced in Release 2.0(1b) are addressed in this section.

Refer to the *Cisco MDS 9000 Family Configuration Guide* and the *Cisco MDS 9000 Family Command Reference.*

The show inventory Command

To view information on the field replaceable units (FRUs) in the switch, including product IDs, serial numbers, and version IDs, use the **show inventory** command.

The error-enabled Command

To enable the error-enabled message display, use the **aaa authentication login error-enable** command.

To disable the error-enabled message display, use the **no aaa authentication login error-enable** command.

To view the current display status, use the **show aaa authentication login error-enable** command.

The snmp-server enable traps Command

To enable a specific SNMP trap (for example, fcdomain traps) notification use the **snmp-server enable traps fcdomain** command.

To disable the specified SNMP trap notification use the **no snmp-server enable traps fcdomain** command.

The Extended ping Command

The **ping** command now provides additional options to verify the connectivity of a remote host or server. To specify these additional parameters, type **ping** at the CLI switch prompt and press **Enter**.

Deprecated Commands

The following commands are deprecated in Cisco SAN-OS Release 2.0(1b):

- The **quiesce interface** and the **quiesce no interface** commands. This functionality is now replaced by the graceful shutdown functionality that is automatically available in all switches in the Cisco MDS 9000 Family (see the "Graceful Shutdown" section on page 9). These commands continue to be available in Cisco SAN-OS Release 1.3.
- The **aaa accounting logsize** and the **no aaa accounting logsize** command. By default about 250 KB of accounting log is automatically displayed.
- The **fcinterop fcid-allocation** command. This command is replaced by the **fcid-allocation area company-id** command.
- The **ip-compression high-throughput** and the **ip-compression high-comp-ratio** commands. Use the **ip-compression mode** (mode 1, 2, 3, or auto) command instead.

Fabric Manager Enhancements

The Cisco MDS 9000 Family Fabric Manager enhancements are as follows:

- Fabric Manager Web Services (to access network management and performance information)
  - Event logs and statistics
  - Historical performance reports
  - Inventory summary reports
  - Administrative capabilities
- Supports enhanced Zoning
- Cisco Fabric Manager physical attributes filtering
- Rearranged Logical and Physical panes
- Displays SANs and multiple fabrics
- Detachable tables in Information pane

- Login screen enhancements
  - Simple versus complex
  - Load from database
  - Can sync server to same NIC as client
- Enclosures in map can bring up customized application when you right-click
- Displays every VSAN island without collapsing them
- LUN IDs are now associated with targets
- FDMI and name server information is collated for initiators (hosts)
- Enclosures are global across SANs
- Performance Manager Wizard enhancements
  - Interpolation
  - Adaptive baseline thresholds
  - Compression
  - Enhanced collection capabilities
- FCIP wizard enhancements
  - Encryption
  - Compression
- FICON enhancements
  - Displays FICON port numbers on map
  - Can assign FICON ports for FCIP PortChannels
- Zoning enhancements
  - Aliases treated as groups
  - Many types of aliases
  - Can rename zonesets, zones, and aliases
  - Backup and restore zone database
  - Enhanced zoning
- Cisco SAN-OS Release 2.0(1b) enhancements also include the following features:
  - DPVM wizard
  - CFS
  - Zone-based QoS
  - IKE/IPsec
  - Port tracking
  - DNS

Device Manager Enhancements

The Cisco MDS 9000 Family Device Manager enhancements are as follows:

- MPS 14/2 support
- AES support (authentication algorithm)
- FCIP interfaces displayed in physical view
- Cisco SAN-OS Release 2.0(1b) enhancements also include the following features:
  - Auto trunk
  - Port tracking
  - DNS
  - Tape acceleration
  - IPS encryption
  - CFS
  - DPVM
- Gigabit Ethernet TCP statistics
- Multicast root
- FCID area allocation
- Additional (and more accurate) flash file manipulation capabilities
- Reads syslog information from the Fabric Manager server
- Summary view enhancements
  - Displays Ethernet PortChannel members
  - Displays the Gigabit Ethernet port associated with FCIP
  - Displays FCIP compression information
- Ability to power down a line card

Refer to the *Cisco MDS 9000 Fabric Manager Guide*.

Limitations and Restrictions

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

- FCIP Links, page 24
- Fabric Manager/Device Manager Support on Windows2003, page 24

Upgrading to Cisco MDS SAN-OS Release 2.0(1b) from Release 1.3(4a)

This procedure applies to Fabric Manager and Device Manager applications using Cisco MDS SAN-OS Release 1.3(4a) software.

To upgrade a switch from 1.3(4a) to 2.0(1b), use Device Manager to copy the image files to bootflash and then use Fabric Manager to perform the upgrade.

To copy the image files from a server or PC to bootflash, follow these steps:

Step 1 Start TFTP, FTP, SCP, or SFTP on the server or PC where you have the image files stored.

Step 2 In Device Manager, select **Admin > Flash Files**. You see the bootflash directory listed for the supervisor's local partition, by default.

Step 3 Select the device and partition from the drop-down lists for the directory containing the file you want to copy.

Step 4 Click the **Copy** button to open the Copy dialog box.

Step 5 Select the protocol you want to use to perform the copy procedure.

Step 6 Enter the address of the source server.

Step 7 If necessary, enter your remote username and password on that server.

Step 8 Click the **...** button after the SourceName field to browse for the source file on your local PC or on the server, depending on the type of copy.

Step 9 Enter the destination name for the file.

Note If you are copying to Flash, the file name must be of the form
[device>:][<partition>:]<file>

where <device> is a value obtained from the Flash device name,
<partition> is obtained from the Flash partition name
and <file> is any character string that does not have embedded colon characters.

Step 10 Click **Apply**.

To upgrade using Fabric Manager, use the Software Install Wizard. Software upgrades may be disruptive under the following conditions:

- A single supervisor system with kickstart or system image changes.
- A dual supervisor system with incompatible system software images.

Note Before you use the Software Install Wizard, verify that the standby supervisor management port is connected.

To use the Software Install Wizard, follow these steps:

Step 1 Open the Software Install Wizard by clicking on its icon in the toolbar.

You see the Software Install Wizard.

Step 2 Select the switches that you want to upgrade or install images from the displayed list.

You must select at least one switch to proceed. When finished, click **Next**.

Step 3 Specify the new images to use for each switch model.

To use images that are already downloaded (the file is already on the bootflash), check the **Skip Image Download** check box.

Step 4 Double-click the table cell under System, Kickstart, or Asm-sfn to see a drop-down list of images to choose from.

Step 5 Select an image to use for the upgrade.

You must select at least one image for each switch to proceed.

Note There is no limit to the number of switches you can upgrade. However, the upgrade is a serial process; that is, only a single switch is upgraded at a time.

Step 6 Start the upgrade.

If you check **version check** before the upgrade process is started, a version check is done. This check provides information about the impact of the upgrade for each module on the switch. It also shows any HA-related incompatibilities that might result. You see a final dialog box at this stage, prompting you to confirm that this check should be performed.

Caution If **version check** is enabled, the upgrade will proceed even if your version is newer than the version you are installing.

Note Before exiting the session, be sure the upgrade process is complete. The wizard will display a status as it goes along. Check the lower left-hand corner of the wizard for the status message `Upgrade Finished`. First, the wizard displays the message `Success` followed a few seconds later by `InProgress Polling`. Then the wizard displays a second message `Success` before displaying the final `Upgrade Finished`.

Refer to the *Cisco MDS 9000 Fabric Manager Guide*.

Temporary User Account

When you log in to a Cisco MDS switch successfully using the Fabric Manager or Device Manager through Telnet or SSH and if that switch is configured for AAA server-based authentication, a temporary SNMP user entry is automatically created with an expiry time of one day. The switch authenticates the SNMPv3 protocol data units (PDUs) with your Telnet/SSH login name as the SNMPv3 user are authenticated by the switch. The management station can temporarily use the Telnet/SSH login name as the SNMPv3 `auth` and `priv` passphrase. This temporary SNMP login is only allowed if you have one or more active MDS shell sessions. If you do not have an active session at any given time, your login is deleted and you cannot perform SNMP v3 operations.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Deleting Roles

If a user only belongs to one of the newly-created roles and that role is subsequently deleted, then the user immediately defaults to the network-operator role.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

The localizedkey Option

Avoid using the **localizedkey** option when configuring an SNMP user from the CLI. The localized keys are not portable across devices as they contain device engine ID information. If a configuration file is copied to the device, the passwords may not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device. Passwords specified with the **localizedkey** option are limited to a 130 characters.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Extended BB_Credit Support

The last two Fibre Channel ports (port 13 and port 14) and the two Gigabit Ethernet ports in the MPS-14/2 module and in the Cisco MDS 9216i Switch do not support the extended BB_credits feature.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

DPVM

The DPVM feature overrides any existing static port VSAN membership configuration. If a device is not configured for a specific VSAN, it continues to be part of the existing port VSAN.

If the VSAN corresponding to the dynamic port is deleted or suspended, the port is shut down.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

PortChannel Autocreation

When enabling autocreation, we recommend that you retain at least one interconnected port between the switches without any autocreation configuration. If all ports between two switches are configured with the autocreation feature at the same time, you may face a possible traffic disruption between these two switches as the ports are automatically disabled and reenabled when ports are added to an autocreated PortChannel.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

IP-ACL Support

Do not apply IP-ACLs to only one member of a PortChannel group. Apply IP-ACLs to the entire channel group.

If IP-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Port Mode for IBM FAStT 500 Storage System

If you are connecting IBM FAStT 500 storage system to Cisco MDS switches, configure the port mode as F instead of Fx or Auto.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

FCIP Links

If the FCIP write acceleration feature or the FCIP compression feature is enabled on an FCIP link, then switches in a fabric running Cisco MDS SAN-OS Release 1.3 will not be compatible with switches in the same fabric running Cisco MDS SAN-OS Release 2.0(1b).

If a Cisco MDS switch running Cisco MDS SAN-OS Release 1.3 is upgraded to Cisco MDS SAN-OS Release 2.0(1b) when FCIP compression or write acceleration is enabled, then an FCIP link failure will occur.

If the upgrade is performed using the Fabric Manager, then the FCIP link continues to remain in the failed state till the connected switches are upgraded.

To avoid this FCIP link failure, disable the write acceleration and the FCIP compression features before beginning the upgrade process.

Fabric Manager/Device Manager Support on Windows2003

Fabric manager/Device manager does not work properly with JRE version 1.4.2_03 on Windows 2003 operating system.

JRE version 1.4.2_05 has been found to work without any issues on Windows 2003.

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

	Software Release (Resolved or Open)	
DDTS Number	**1.3(5)**	**2.0(1b)**
Severity 1		
CSCeg13762	O	R
CSCeg33121	O	O
Severity 2		
CSCed57251	O	O
CSCef65409	O	R
CSCef83504	O	R
CSCef86223		O
CSCef89511		O
CSCef93586		O
CSCef97057		O
CSCef98143		O
CSCeg02834		O
CSCeg06512		O
CSCeg07325		O
CSCeg07339		O
CSCeg09210		O
CSCeg12962		O
CSCeg17593		O
CSCeg18886	O	R
CSCeg20932		O
CSCeg23889	O	O
CSCeg30690		O
CSCeg33732		O
CSCeg44018		O
CSCeg53094		O
CSCeg58996		O
CSCeh61610	O	O
CSCeh96928	O	O
CSCei25319	O	O
CSCsd78967	–	O

Table 3 Release Caveats and Caveats Corrected Reference (continued)

DDTS Number	Software Release (Resolved or Open)	
	1.3(5)	2.0(1b)
CSCsh27840	O	O
Severity 3		
CSCec31365	O	O
CSCed14920	O	O
CSCed20053	O	O
CSCef56229		O
CSCef70000	O	R
CSCef74578		O
CSCef82882		O
CSCef91854		O
CSCef94903		O
CSCef95611		O
CSCef96472		O
CSCeg01545		O
CSCeg01551		O
CSCeg02245		O
CSCeg05450		O
CSCeg12383		O
CSCeg20292		O
CSCeg24199		O
CSCeg37598		O
CSCeg46989		O
CSCeg53114		O
CSCeg56197	O	O
CSCeg59198		O
CSCeg61535	O	O
CSCeg66225		O
CSCeg81089		O
CSCeg85146		O
CSCeh19639		O
CSCeh21199	O	O
CSCeh41099		O
CSCeh51924		O
CSCeh52280		O
CSCeh56143		O

Table 3 Release Caveats and Caveats Corrected Reference (continued)

	Software Release (Resolved or Open)	
DDTS Number	**1.3(5)**	**2.0(1b)**
CSCeh64080	O	O
CSCeh65824		O
CSCeh82490		O
CSCeh83514		O
CSCeh87985		O
CSCei67982		O
CSCei91676	O	O
CSCei91968		O
CSCin81760	O	R
CSCin81851		O
CSCsc31424		O
CSCsc33788	O	O
CSCsf21970	–	O
CSCsg03171	–	O
Severity 4		
CSCeh42252	O	O

Resolved Caveats

- CSCeg13762

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

  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).

- 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).

- 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.

- CSCeh52280

  Symptom: A corrupted license file installs on an MDS 9000 switch without errors.

  Workaround: None.

- CSCeh56143

  Symptom: A Fabric Manager zone migration wizard causes a Telnet session to hang when a non-MDS switch is present.

  Workaround: None.

- CSCeh64080

  Symptom: Following an upgrade from Release 1.1 to Release 1.3 or higher, with persistent FC ID enabled, the FC IDs for the storage arrays may get changed after a link flap.

  Workaround: None.

- CSCeh65824

  Symptom: If you install an SSM and boot it with either the VSFN or SSI Image, the Enterprise License grace period starts.

  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.

Open Caveats

- CSCeg33121

  Symptom: A small amount of memory in the IP configuration process leaks each time any of the following commands execute: **show running-config**, **show startup-config**, **copy running-config startup-config**. After repeated occurrences, the command fails to execute.

  Workaround: None.

- 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.

- CSCef86223

  Symptom: The IPsec feature supports 100 simultaneous encrypted tunnels for each Gigabit Ethernet interface. If you exceed this limit, the port fails.

  Workaround: None.

- CSCef89511

  Symptom: When you disable in-order delivery in a Cisco MDS 9000 Family switch, and if you change the default zone's priority in the presence of an active zoneset, then the packets with the old priority may arrive out of order.

  Workaround: None.

- CSCef93586

  Symptom: If you insert or reboot a standby supervisor while the active is in steady state, you may see the following message before the standby supervisor goes online under certain circumstances:

  2004 Oct 4 20:45:39 sw172 %KERN-2-SYSTEM_MSG: do_xmit_sync_msgs() returned -70 (aipc): msg_id=0x2deeb, msg_num=1, data_size=60, msg_size=108, skb_size=170

  After issuing this message, the active supervisor module forces another reboot of the standby supervisor module and prints the following syslog message

  %SYSMGR-2-SYNC_FAILURE_STANDBY_RESET).

  This double reboot takes a longer time for the standby supervisor module to go online. It does not impact the stability of the system. Once the standby supervisor is online, this problem cannot occur.

  Workaround: None.

- CSCef97057

  Symptom: When the nWWN of a device logged through a port is assigned a new VSAN, and when the DPVM database is activated, then the port does not move to the new VSAN.

  Workaround: Disable and enable the interface.

- CSCef98143

  Symptom: When the fabric is in the enhanced zoning mode and if a new inter-switch link (ISL) triggers a zone database merge failure, then the commands to export/import the zone database fail to bring up the link.

  Workaround: Fix the databases and then bring up the links in the switches on either side of the link.

- CSCeg02834

  Symptom: While downgrading from Cisco MDS SAN-OS Release 2.0(1b) to Cisco MDS SAN-OS Release 1.3(x), if the CIM server is enabled, the Gigabit Ethernet ports may go down.

  Workaround: Disable the CIM server when downgrading from 2.0(1b) to 1.3(x)

- CSCeg06512

  Symptom: The iSNS server fails if you disable the iSNS server when the initiator is configured on the local switch, registers with the remote switch, and logs into the available targets on both switches.

  Workaround: None.

- CSCeg07325

Symptom: If a new VSAN is added to the TE port channel after a hitless upgrade to Cisco MDS SAN-OS Release 2.0(1b), any new vsans brought up in this port channel will either not come up or will come up, but not carry any traffic. This will also appear in following situations after the upgrade to release 2.0(1b):

a. Suspend an active VSAN on the TE port channel and then unsuspend

b. Clear an active VSAN from the TE port channel and then add it back.

c. A brand new vsan is added/created on the switch

Workaround: There are two workarounds for these issues:

a. Issue the **shutdown/no shutdown** command sequence on the TE port channel once.

b. Reset all but one member of the port channel. When these reset members come back up, reset the last remaining member. This will ensure that the port channel remains operationally up, while resolving the problem.

- CSCeg07339

  Symptom: The iSCSI/IPSec session may go down and come back up after a few hours if using Microsoft's implementation of IPsec in the iSCSI initiator software.

  Workaround: None.

- CSCeg09210

  Symptom: In some cases the FICON port attributes will show no attributes in Device Manager.

  Workaround: None.

- CSCeg12962

  Symptom: Some hosts may not accept IKE tunnel creation from Cisco MDS switches when an IKE session already exists in the Cisco MDS switch. In such cases it may take more than the expected time for the IPsec session to come up. This scenario can happen when the Gigabit Ethernet interface on the Cisco MDS switch fails and comes back up or if you issue a VRRP switchover to a different Cisco MDS switch.

  Workaround: For a faster recovery, disconnect and re-initiate the iSCSI session from the host.

- CSCeg17593

  Symptom: The zone server might fail to read its configuration because of some inconsistent values in its configuration during an upgrade.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 2.0(2b).

- CSCeg20932

  Symptom: If an IPS module with operational FCIP PortChannels is reloaded, upgraded, or downgraded, the supervisor module may be reloaded causing the system to reboot.

  Workaround: Before reloading, upgrading, or downgrading an IPS module, shut down all FCIP PortChannels on the line card.

- 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.

- CSCeg30690

  Symptom: The SAN extension tuner tool cannot be used to inject traffic on FCIP links that have write acceleration enabled.

  Workaround: None.

- CSCeg33732

  Symptom: The SNMP process might fail under certain error conditions if you are adding a member to a zone using fcalias type.

  Workaround: None.

- CSCeg44018

  Symptom: Sometimes in-service software upgrades from previous releases to Release 2.0(1b) causes errors in FICON VSANs showing up as IFCC errors on mainframe.

  Workaround: None.

- CSCeg53094

  Symptom: The XIOTECH initiator does not recognize remote storage devices.

  Workaround: Issue the fcid-allocation area company-id 0x00d0b2 command before connecting the devices to the switch to ensure that the storage devices get FCIDs with a unique area byte. If the devices are already connected, refer to the Cisco MDS 9000 Family Configuration Guide for information about adding a company-id to the list.

- CSCeg58996

  Symptom: Scheduled jobs are sometimes executed twice in a day.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 2.0(3)

- CSCeh49026

  Symptom: The application might report that the loop port is not up, however, the port is online and operational.

  Workaround: Issue the shutdown/no shutdown command sequence to clear the problem.

- CSCeh61610

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

  Workaround: None.

- CSCeh96928

  Symptom: If your switch port is configured in auto speed (switchport speed auto) and auto mode (switchport mode auto), the switch-port fails to establish a link with the device connected through Emulex HBA LP8000 and remains in link-failure state. The problem occurs with the following combination of HBA, Driver, Firmware, and OS configured at 1 Gbps.

  Workaround: Configure the switch port speed to 1 Gbps (switchport speed 1000) to support the Emulex HBA LP8000.

- CSCei25319

  Sympton: 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.

- CSCsd78967

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

- 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.

  Workaround: None.

- CSCec31365

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

  Workaround: None.

- CSCed14920

  Symptom: During a switch upgrade, a SAN Volume Controller (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 is `unconfigured`.

  – The `node state` of the affected SVC node is `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.

- CSCef56229

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

  Workaround: None.

- CSCef74578

  Symptom: When the bit error rate exceeds a threshold, the switch does not send out the RLIR frame correctly.

  Workaround: Upgrade to Cisco MDS SAN-OS Release 2.0(2b).

- CSCef82882

  Symptom: A VSAN restricted user can change the assignment of a VSAN for an Fx port and have access to other VSANs using SNMP.

  Workaround: None.

- CSCef91854

  Symptom: If a number of DPVM device entries are deleted together (by highlighting them) from the Fabric Manager or the Device Manager, these entries are not deleted properly.

  Workaround: The workaround for this problem is to delete one DPVM device entry at a time.

- CSCef94903

  Symptom: IPACL rules are deleted from the running configuration when issuing the **show startup configuration** command. Issuing the following commands might result in losing all the ipacl rules:

  – **show startup**

  – **copy running** to **startup**

  – **reload**

  Workaround: Upgrade to Cisco MDS SAN-OS Release 2.0(2b).

- CSCef95611

  Symptom: After a successful database merge, the output of the **show cfs merge status name** *application_name* command may not reflect the correct merge status. However, the merge operation remains successful.

  Workaround: None. The correct status is displayed when you perform additional CFS operations.

- CSCef96472

  Symptom: The boot variables are not visible in the output of the **show startup-config** command. However, the boot variables are successfully saved in startup configuration and are applied at the next switch reboot. This impact occurs only if you use the following sequence:

  a. Copy the startup configuration to a file.

  b. Issue the **write erase boot** command to erase the boot variables.

  c. Copy the saved file back to the startup configuration.

  Workaround: If you use the specified sequence, manually set the boot variables.

- CSCeg01545

  Symptom: If you issue a blank commit after merge failure or if this is the first commit after merge failure, the current config database is activated in all switches in the fabric. If the config database is null or made null, then the database is deactivated in all switches.

  Workaround: None.

- CSCeg01551

  Symptom: If you issue a **commit** command, the DPVM application implicitly activates the existing configuration database. The configuration database is activated only when the **commit** command is explicitly issued after the **activate** command.

  Workaround: None.

- CSCeg02245

  Symptom: After creating or deleting VSANs, the Fabric Manager client does not list the VSANs correctly.

  Workaround: Reopen (click on **File** > **Open Fabric** or the **Open Fabric** toolbar button) to display an accurate list of VSANs.

- CSCeg05450

  Symptom: In Device Manager, ports which dynamically become member of the FICON VSAN are not visible. Only static FICON VSAN ports are displayed.

  Workaround: Make static and dynamic port VSANs identical.

- CSCeg12383

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

  Workaround: Reconfigure the switchport trunk mode on the PortChannel.

- CSCeg20292

  Symptom: Issuing the **Ctrl-Z** sequence in the command-line interface does not exit configuration submode.

  Workaround: Type **exit** command to exit the configuration submode.

- CSCeg37598

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

  Workaround: None.

- CSCeg46989

  Symptom: The **copy running-configuration startup-configuration** command fails to save the **zone default-zone permit vsan xx** command. In FICON environments, importing a configuration from one switch without this line, may prevent the data to flow as there are no real zones except the default zone.

  Workaround: Add “zone default-zone permit vsan xx" in the configuration when applying the configuration to a different switch.

- CSCeg53114

  Symptom: WWNs assigned to iSCSI initiators by the system can inadvertently be returned to the system when an upgrade fails or a manual downgrade is performed, such as when an older iSAN software version is booted up without using the **install all** command. In these scenarios, the system can later assign those WWNs again to other initiators, which causes conflicts. This bug is a duplicate of CSCei17870.

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

  Workaround: None

- CSCeg59198

  Symptom: If your host or management application is configured to receive notifications from a Cisco MDS 9000 Family switch using SNMPv1, the source address of the notification might not contain the IP address of the switch. As a result, the host may not interpret the notification properly.

  Workaround: Use SNMPv2c or upgrade to Cisco MDS SAN-OS Release 2.0(3).

- 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.

- CSCeg81089

  Symptom: A Windows host running Hummingbird 10 with Connectivity Secure Shell 9, cannot use SSH to connect to an MDS switch running Cisco MDS SAN-OS Releases 2.0(x)using the same host configuration as was used when connecting to an MDS switch running 1.3(x) code.The host will display the error, "Authentication Failed, no more shared authentication methods".

  Workaround: Reconfigure the client to use "keyboard-interactive" instead of "password" for authentication. To do this, go to tunnel profile settings, select Security Settings>Authentication. Ensure the "keyboard interactive" is the method used, "password" might be the currently configured method. Or upgrade to Cisco MDS SAN-OS Release 2.1(1a).

- CSCeg85146

  Symptom: The **show running** command shows the callhome profile alertgroups with an underscore (_) rather than a dash (-). If the **show running** command in Cisco MDS SAN-OS Release 1.3.x shows callhome profile with alertgroups as an underscore (_), then it will carry it over to the release 2.0.x code and cannot be deleted. This occurs if the following alert groups have been configured:

  - cisco_tac
  - supervisor_hardware
  - linecard_hardware

  Workaround: Before upgrading to Cisco MDS SAN-OS Release 2.x, issue the **show running** command and delete the following alert groups:

  - cisco_tac
  - supervisor_hardware
  - linecard_hardware

- CSCeh19639

  Symptom: Alias for a down endport is not shown andis referenced by its pwwn in the Edit FullZoneset screen of the Fabric Manager rather than the fcalias name. This does not affect the functionality of adding those members to the zones either in Fabric Manager or in the CLI.

  Workaround: None

- 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).

- CSCeg24199

  Symptom: Your connection to the server might terminate during an upgrade/downgrade process if the client is detecting the server's status upon receiving events. If the client does not receive any events from the server for a certain amount of time, it assumes that the server is down and closes the connection. Fabric Manager timeouts have also been seen that do not coincide with upgrade/downgrade events.

  Workaround: Remove the fabric and then reopen it.

- CSCeh41099

  Symptom: Protocol and port numbers, if specified in a IP ACL assigned to a IPSec profile (crypto map), will be ignored.

  The interop between Microsoft's iSCSI initiator with IPSec encryption with Cisco MDS 9000 Series switches. If IPSec is configured in the Microsoft iSCSI initiator (also the IPSec/IKE initiator), the host IPSec implementation sends the following IPSec policy:

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

  Upon receiving the above policy, the protocol and port numbers are ignored and only the IP addresses for the IPSec policy are used. Thus, althhough iSCSI traffic is encrypted, non-iSCSI trafffic (such as ICMP ping) sent by the Microsoft Host in cleartext will be dropped in the MDS port.

  Workaround: None.

- CSCeh51924

  Symptom: A corrupted entry is created in the snmpTargetParamsTable when a user creates an entry with NULL string in object snmpTargetParamsName as its index. The SNMP service may stop and restart.

  Workaround: None. To avoid similar problems, enter a name in snmpTargetParamsName with at least one character when creating a snmpTargetParamsEntry.

  Workaround: None

- 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.

- CSCei67982

  Symptom: During an upgrade of an MDS switch with two or more MPS-14/2 modules, FCIP tunnels on multiple MPS-14/2 modules can be down at the same time. If a PortChannel of two FCIP tunnels on different MPS-14/2 modules is used for redundancy, the redundancy can be lost. If IVR is running over these FCIP tunnels, IVR can lose remote devices as a result of loss of access over the FCIP based PortChannel.

  Workaround: Place other modules on which you can perform a hitless upgrade between the MPS-14/2 modules to allow for more time between module upgrade and to give the FCIP tunnels more time to stabilize. To recover access over the FCIP based PortChannel, reactivate the IVR zone set by adding a dummy zone with two dummy members.

- 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.

- CSCei91968

  Symptom: In a fabric with more than one switch, there is a possibility of CFS or syslog crashing because of a PSS-FULL condition. This happens because of leakage in the PSS records stored by the CFS module.

  CFS internal distributions cause a PSS leakage during one of the following:

  - An application registration/de-registration. (This is at the rate of 1 PSS records or 60 bytes per event.)
  - -An ISL Link flap. (This is at the rate of 2 PSS records per CFS registered application. For 10 CFS registered applications, a 1000 flaps would cause a leak of about 1M.)

  Application and Regular CFS distributions in a stable fabric do not result in PSS leakages.

  Workaround: None. A switchover will help in cleaning up these records but the usage of the partition remains same (dev/shm partition). However, CFS will reuse the freed space for further PSS storage.

- CSCin81851

  Symptom: A system switchover causes the boot variables to disappear from display in both the **show running** and **show startup** command outputs. However, the functionality is unaffected, and the boot variables are still set as displayed in the **show boot** command output.

  Workaround: Issue the **show boot** command to verify the boot variables.

- CSCeh82490

Symptom: An MDS 9000 switch running SAN-OS 2.0(1b) can potentially send excessive Call Home messages due to a malfunctioning line card that acts as if it were being inserted and removed repeatedly.

Workaround: None.

- CSCeh83514

  Symptom: After upgrading to Release 2.0, it is no longer possible to create, modify, or delete the admin role.

  Workaround: Before upgrading to Release 2.0, create the admin role.

- CSCeh87985

  Symptom: When no role is associated with a user, SNMP fails when the **no role name admin** command is issued to delete the admin role. The SNMP user (admin) has no roles assigned, which causes the failure when there is an attempt to delete a specific role.

  Workaround: Associate at least one role (group) to the user by executing the **snmp-server user** *username* [*group-name*] command in config mode.

- CSCsc31424

  Symptom: Issuing the **no shutdown** command on a port produces this error:

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

  You can reproduce the problem by removing a port from a port channel and then perform a system switchover. However, the problem does not always occur with these steps.

  Workaround: Use the **channel-group X** command where port channel X, to configure a new port channel and add the port to it. Then use the **no interface port-channel X** command to remove the newly created port channel. The **no shutdown** command will now be accepted on the port.

- 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.

- CSCsf21970

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

Workaround: Wait 5 seconds between the delete and the following create command for a given FCIP interface.

- CSCsg03171

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

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

- 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:

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9000 Family Software Upgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric and Device Manager Online Help*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

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_inpck/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.

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.

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.

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

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