Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.0(2a)

CCO Date: February 5, 2005

Text Part Number: OL-3855-01 A0

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 11.

Note Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

Table 1 shows the on-line change history for this document.

Table 1 On-Line History Change

Revision	Date	Description
A0	06/23/2005	Added DDTS CSCei25319

Contents

This document includes the following section:

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

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.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 1.0(2a) and includes the following topics:

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 3.

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

Component	Part Number	Description	Applicable Products
Software	M9500-SF1EK9-1.0.2	MDS 9500 supervisor/fabric-I, enterprise software	MDS 9509 only
	M9200-EK9-1.0.2	MDS9216 enterprise software	MDS 9216 only
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot chassis, dual 2500W AC power supplies, and dual supervisors — SFPs sold separately)	MDS 9509 only
	DS-C9216-K9	MDS 9216 16-port modular fabric switch (includes sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot — SFPs sold separately)	MDS 9216 only
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 supervisor/fabric-I, module	MDS 9509 only
Switching modules	DS-X9016	MDS 9000 16-port 1/2-Gbps Fibre Channel module (SFPs sold separately)	MDS 9509 and 9216
	DS-X9032	MDS 9000 32-port 1/2-Gbps Fibre Channel module (SFPs sold separately)	

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

Component	Part Number	Description	Applicable Products
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	1/2-Gbps Fibre Channel — short wave SFP	MDS 9509 and 9216
	DS-SFP-FC-2G-LW	1/2-Gbps Fibre Channel — long wave SFP	
Power supplies	DS-CAC-845W	AC Power supply for MDS 9216	MDS 9216 only
	DS-CAC-2500W	2500W AC power supply	MDS 9509 only
	DS-CAC-4000W-US	4000W[2] AC power supply for US (cable attached)	
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CDC-2500W	2500W DC power supply	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB	MDS 9509 only

1. SFP = small form factor pluggable
2. W = Watt

Determining the Software Version

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

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

Feature Set

This Cisco MDS SAN-OS Release 1.0(2a) software is packaged in feature sets (also called software images) depending on the platform. The Cisco MDS SAN-OS software feature sets available for the Cisco MDS 9000 Family include Ethernet, Fibre Channel (1 Gbps and 2 Gbps), SNMP, and IP packets.

New Features in Release 1.0(2a)

SAN-OS Release 1.0(2a) is a maintenance release for switches in the Cisco MDS 9000 Family. See the "Caveats" section on page 5 for details on closed and outstanding caveats and limitations.

Boot Loader Upgrade for the Active Supervisor Module

SAN-OS Release 1.0(2a) introduces changes to the boot loader upgrade procedure for the active supervisor module.

This procedure does not affect traffic and can be issued at any time.

Note If the boot loader is upgraded, you need to reboot to make the new boot loader effective. You can schedule the reboot at a convenient time so traffic will not be impacted.

To initialize and verify the kickstart image in an active supervisor module, follow these steps:

Step 1 Download the kickstart image to the supervisor module as the URI

Step 2 Issue the **init bootloader** command to program the boot loader.

```
switch# init bootloader bootflash:kick-1.0.2
Extracting bootloader
Installing bootloader
```

Note The file name for the kickstart image may differ based on your naming convention or setup. Use the relevant file name that applies to your setup.

Step 3 Use the **dir bootflash:** command to verify that the BIOS was programmed correctly (optional).

```
switch# dir bootflash:
admin    18839862  Jan 01 22:32:02 1980 isan-1.0.2
admin    14558720  Jan 01 22:33:32 1980 kick-1.0.2 <----------------------------kickstart image
root        12288  Dec 22 23:32:06 2002 lost+found
```

Note The URI is always the kickstart image URI in the supervisor module.

Limitations and Restrictions

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

- FCC, page 4
- Install Command, page 4
- RADIUS, page 5

FCC

Fibre Channel Congestion Control (FCC) is a Cisco proprietary flow control mechanism that alleviates congestion on Fibre Channel networks. FCC reduces the congestion in the fabric without interfering with the standard Fibre Channel protocols. The FCC protocol increases the granularity and the scale of congestion control applied to any class of traffic.

Testing is in progress for this feature. It is not supported for this release.

Install Command

SAN-OS Release 1.0(2a) does not support the **install all** command.

RADIUS

If the timeout values and/or the retry count of the RADIUS server is too large, you may not be able to login into the system if the RADIUS servers are down.

Be sure to have a reasonable timeout and retry count. The cumulative response or timeout latency from RADIUS servers should not be more than 50 seconds. For example, in the following configuration:

radius server timeout 5
radius server retransmit 3
radius server host A
radius server host B
The worst case cumulative response or timeout latency for this example is:
(5+1)*3 + (5+1)*3 = 36

Add 1 (one) to the retransmit count before calculating the total count (number of tries = number of retransmits + 1).

Another option is to have multiple RADIUS servers to backup a server that has gone down.

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, "C" indicates a closed caveat, and "O" indicates an open caveat.

Table 3 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release 1.0(1) Closed or Open	Software Release 1.0(2) Closed or Open	Software Release 1.0(2a) Closed or Open
Severity 2			
CSCdz49739	O	C	C
CSCdz47813	O	C	C
CSCdz40286	O	O	O
CSCdz49589	O	O	O
CCSdz31332	O	O	O
CSCdz41824	O	O	O
CSCdz62706		O	O
CSCdy66634		O	O
CSCea11544			C
CSCei25319	O	O	O
Severity 3			
CSCdz40837	O	C	C
CSCdz39137	O	C	C
CSCdz38419	O	C	C
CSCdz25873	O	C	C

Table 3 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release 1.0(1) Closed or Open	Software Release 1.0(2) Closed or Open	Software Release 1.0(2a) Closed or Open
CSCdz42206	O	C	C
CSCdz39924	O	C	C
CSCdz40770	O	C	C
CSCdz34906	O	C	C
CSCdz16649	O	C	C
CSCdz30806	O	O	O
CSCdy71186	O	O	O
CSCdz38248	O	O	O
CSCdy77777	O	O	O
CSCdz40221	O	O	O
CSCdz29899	O	O	O
CSCdz36297	O	O	O
CSCdz41155	O	O	O
CSCdz42325	O	O	O
CSCdz41227	O	O	O
CSCdz76025		O	O
CSCdz73481		O	O
CSCdz73186		O	O
CSCdz62711		O	O
CSCdz80007		O	O
CSCdz81955		O	O
CSCdz12179		O	O
CSCdz80310			C

Closed Caveats

- CSCea11544

  Symptom: Reachability is impacted in a VSAN that is created or updated on a switch that has been active for a month.

  The FSPF counter overflows in a switch that has been active for a month. As a result, when a user either creates or updates a VSAN on this switch, the reachability to and from this VSAN is impacted. This problem does not impact other VSANs.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea11544

- CSCdz80310

  Symptom: An HDS 9970 Truecopy initiator port sends a RFT_ID in a 12-byte field, when it should be in a 32-byte field. Cisco MDS 9000 Family switches reject this payload and the initiator halts.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSC80310

Open Caveats

- CSCdz40286

  Symptom: When VSAN interfaces (VNI) are present in a system, you may receive some extra RSCNs when a system switchover is performed.

  Workaround: None.

- 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.

- CSCdz30806

  Symptom: When you copy a file from active bootflash: to standby bootflash: and if the space available on standby bootflash: is insufficient to store the copied file, the **copy** command may report a success even though the file has not been copied to standby bootflash:.

  Workaround: Always verify if sufficient disk space is available on the standby bootflash: before attempting to copy a file from one bootflash: to another.

- CSCdy71186

  Symptom: When you bring down a range of FL ports, there is a delay of four (4) seconds. This problem does not affect switch operation.

  Workaround: None.

- CSCdz38248

  Symptom: SyslogServerAddressType setting is not preserved across switch resets, when configured using the Cisco Fabric Manager tool.

  Workaround: None.

- CSCdy77777

  Symptom: When a fcsDiscoveryCompleteNotify trap is received through the nlmLog table, the fcsVsanDiscoverName is missing.

  Workaround: None.

- CSCdz40221

  Symptom: Using the Element Manager or the Fabric manager, administrators can download an image to slot0 even though there is no flash in slot0.

  Workaround: None.

- CSCdz29899

  Symptom: FLOGI ACC(s) sent out on FL ports are not spanned.

  If an FL port is configured as a SPAN source, the FLOGI accepts that leave this FL port are not spanned to the SPAN destination.

  Workaround: None.

- CSCdz36297

  Symptom: If the standby supervisor bootflash does not have sufficient space for a new image, auto synchronization fails. This failure leaves a partial image file on the standby bootflash.

  Workaround: Delete all unnecessary files from the standby bootflash and make room for the new image.

- CSCdz49589

  Symptom: In the Cisco Fabric Manager, when you right click on a standby supervisor module and select **Reset**, the standby supervisor module powers-down instead of power-cycling.

  Workaround: To reset the standby module from the Cisco Fabric Manager, select the **Reset Switch** option in the **Admin** pulldown. In the resulting dialog box, click the **Reset Standby** button

- CSCdz41155

  Symptom: The **show logging level** command does not display the configured levels for some MDS services like system manager, RDL, and FLOGI.

  Workaround: None.

- CCSdz31332

  Symptom: If automatic image synchronization is enabled, and the standby supervisor module is synchronizing the image from the active supervisor, the switch won't stop the user from issuing the **reload** command on the active or standby supervisor modules. This may result in a failure to synchronize the images.

  Workaround: Be sure to allow sufficient time for the images to be synchronized before reloading a supervisor module.

- CSCdz41824

  Symptom: If the timeout values and/or the retry count of the RADIUS server is too large, you may not be able to login into the system if the RADIUS servers are down.

  Workaround: Be sure to have a reasonable timeout and retry count. The cumulative response or timeout latency from RADIUS servers should not be more than 50 seconds (see the "RADIUS" section on page 5).

  Another option is to have multiple RADIUS servers to backup a server that has gone down.

- CSCdz42325

  Symptom: When the switch boots for the first time and you configure the initial setup dialogue, or if you issue the **write erase** command and then reboot the switch, the setup process creates the configuration based on the input that you provide for the configuration. If a command execution goes wrong at this stage, it displays the following error:

  ```
  Error: There was an error executing at least one command
  Please verify the running configuration of the switch.
  ```

  In some cases, this error is not reported. For example, if an IP address is configured on the network, the error may not be reported.

  Workaround: Verify that the applied config is accurate by issuing a **show running-config** command.

- CSCdz41227

  Symptom: When you enter the IP address for the FC analyzer, save the configuration, and reboot the switch you will loose the remote capture configuration.

  ```
  switch(config)# fcanalyzer remote ip-address
  switch# copy running-config startup-config
  switch# reload
  This command will reboot the system. (y/n)? y
  ```

  Workaround: To perform a remote capture on restart or on switchover remove and add the host to the remote host list.

- CSCdz62706

  Symptom: When a zoning configuration change is made while a switch is powering-up, some entries may be rejected and a *lock busy* error message is generated.

  Workaround: Re-enter the configuration after the E-port comes up.

- CSCdz76025

  Symptom: SW-RSCN frames sent by the switch may contain non-zero values in the reserved field. While this field is ignored by the receiving Cisco MDS 9000 Family switches, other vendor switches may respond otherwise.

  Workaround: None.

- CSCdz73481

  Symptom: Cisco MDS 9000 Family switches support multi-pid RSCN from 1.0(2a). In some cases, it may send out more than one SW-RSCN, when the option is turned on for the same event (port_online).

  Workaround: None.

- CSCdz73186

  Symptom: When interoperating using a Cisco MDS 9000 Family switch and a Brocade 3900 switch, the zonesets on the MDS switch and Brocade 3900 switch may be out-of-sync due to a non-standard timeout used by the 3900 device.

  Workaround: None.

- CSCdz62711

  Symptom: Currently a boot variable image does not check platform compatibility.

  This is an enhancement request. When enhanced, the image specified in the **boot** command will be checked against the platform to verify that the image can run on the current platform. That is, an MDS 9500 image runs on the MDS 9500 switch and an MDS 9200 image runs on the MDS 9200 switch.

  Workaround: None.

- CSCdz80007

  Symptom: After rebooting and performing a switchover on a dual supervisor switch, it is possible that a VSAN may display an `up` operational state even if that VSAN may not contain any ports or if none of the ports in that VSAN are up.

  This can cause the Fabric Manager to continuously try fabric discovery on this VSAN and to ultimately timeout with an error.

  Workaround: Change the administration state of the VSAN to `suspended` and bring it back to `active`. Doing so will correct the operational state of the affected VSANs.

- CSCdz81955

  Symptom: CLI command output attachment in XML Call Home messages are not XML encoded. In most cases it does not cause problems, as the special characters (which should be used with appropriate encoding, for example: > or <) do not appear in CLI command output. In some cases where stack traces are attached (as a result of a process crash), the CLI command output may contain these characters. These characters break the XML parsing in the back end.

  Workaround: Contact the Technical Assistance Center (see the "Obtaining Technical Assistance" section on page 12).

- CSCdy66634

  Symptom: When using the Fabric Manager on Solaris or Linux platforms, if you access a parent menu the submenus start disappearing. This is a known Java bug.

  Workaround: For more details access the Java website: http://developer.java.sun.com/developer/bugParade/bugs/4470374.html.

- CSCdz12179

  Symptom: When the Fabric Manager or Device Manager is run through VPN or any NAT scheme, a generic error 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.

Related Documentation

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Cisco MDS 9200 Series Hardware Installation Guide

Cisco MDS 9500 Series Hardware Installation Guide

Cisco MDS 9000 Family Configuration Guide

Cisco MDS 9000 Family Command Reference

Cisco MDS 9000 Family Fabric Manager User Guide

Cisco MDS 9000 Family Troubleshooting Guide

Cisco MDS 9000 Family System Messages Guide

Cisco MDS 9000 Family MIB Reference Guide

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, network services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **E-mail** option under the "Leave Feedback" at the bottom of the Cisco Documentation home page.

You can e-mail your comments to mdsfeedback-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4) —You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3) —Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2) —Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1) —Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a case is automatically opened.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.