

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

# Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.3(3c)

**Release Date:** April 14, 2004

**Text Part Number:** OL-4959-04 Rev. Q0

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 17.



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](http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html)

[Table 1](#) shows the on-line change history for this document.

**Table 1** On-Line Change History

| Revision | Date       | Description   |
|----------|------------|---|
| A0       | 8/12/2004  | Added DDTS <a href="#">CSCed44067</a> .   |
| B0       | 8/26/2004  | Added the <a href="#">Limitations and Restrictions</a> section to include the limitation about Upgrading to Release 1.3(3). |
| C0       | 9/2/2004   | Added DDTS <a href="#">CSCed64425</a> .   |
| D0       | 11/9/2004  | Added DDTS <a href="#">CSCef83504</a>   |
| E0       | 12/4/2004  | Added DDTS <a href="#">CSCee01143</a> .   |
| F0       | 12/08/2004 | Added DDTS <a href="#">CSCin81760</a>   |
| G0       | 12/22/2004 | Added DDTS <a href="#">CSCeg61535</a>   |
| H0       | 01/14/2005 | Added DDTS <a href="#">CSCeg56197</a> .   |
| I0       | 01/21/2005 | Modified DDTS <a href="#">CSCee06496</a>  |
| J0       | 02/22/2005 | Added DDTS <a href="#">CSCee89946</a> , <a href="#">CSCee04343</a> , <a href="#">CSCee54650</a>                             |



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

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

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

**Table 1**      **On-Line Change History (continued)**

| Revision | Date       | Description   |
|----------|------------|---|
| K0       | 03/24/2005 | Added DDTs <a href="#">CSCed36114</a> , <a href="#">CSCed20053</a> , <a href="#">CSCed42077</a> , <a href="#">CSCed51574</a> , <a href="#">CSCed58155</a> , <a href="#">CSCed65607</a> , <a href="#">CSCed75825</a> , <a href="#">CSCed94302</a> , <a href="#">CSCed96246</a> , <a href="#">CSCee43249</a> , <a href="#">CSCeg13762</a> , <a href="#">CSCeh21199</a><br>Removed DDTs <a href="#">CSCdz12179</a> . Resolved in previous release. |
| L0       | 05/31/2005 | Added DDTs <a href="#">CSCeh42252</a> and <a href="#">CSCeg66225</a>  |
| M0       | 06/23/2005 | Added DDTs <a href="#">CSCei25319</a>   |
| N0       | 07/29/2005 | Added DDTs <a href="#">CSCed57251</a> and <a href="#">CSCec31365</a>  |
| O0       | 05/01/2006 | Added DDTs <a href="#">CSCeg84871</a> , <a href="#">CSCei91676</a> , and <a href="#">CSCej08751</a>   |
| P0       | 06/06/2006 | Removed DDTs <a href="#">CSCed16845</a> .   |
| Q0       | 02/26/2007 | Added DDTs <a href="#">CSCsh27840</a> .   |

## Contents

This document includes the following section:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [Image Upgrade, page 5](#)
- [New Features in Release 1.3\(3c\), page 5](#)
- [Limitations and Restrictions, page 5](#)
- [Caveats, page 5](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation, page 18](#)
- [Documentation Feedback, page 19](#)
- [Cisco Product Security Overview, page 20](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 22](#)

## Introduction

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

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

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

# System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 1.3(3c) and includes the following topics:

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

## Hardware Supported

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

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

| Component          | Part Number     | Description   | Applicable Products      |
|--------------------|-----------------|---|--------------------------|
| Software           | M95S1K9-1.3.3c  | MDS 9500 Series supervisor/fabric-I, enterprise software  | MDS 9500 Series only     |
|                    | M92S1K9-1.3.3c  | MDS 9216 enterprise software  | MDS 9216 only            |
|                    | M91S1K9-1.3.3c  | MDS 9100 Series enterprise software   | MDS 9100 Series only     |
| Chassis            | DS-C9509        | MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately) | MDS 9509 only            |
|                    | DS-C9506        | MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately.                     | MDS 9506 only            |
|                    | DS-C9216-K9     | MDS 9216 16-port semi-modular fabric switch (includes sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately)          | MDS 9216 only            |
|                    | DS-C9120-K9     | MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports)   | MDS 9120 only            |
|                    | DS-C9140-K9     | MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports)   | MDS 9140 only            |
| Supervisor modules | DS-X9530-SF1-K9 | MDS 9500 supervisor/fabric-I, module  | MDS 9500 Series only     |
| Switching modules  | DS-X9016        | MDS 9000 16-port 2/1-Gbps Fibre Channel module (SFPs sold separately)   | MDS 9500 Series and 9216 |
|                    | DS-X9032        | MDS 9000 32-port 2/1-Gbps Fibre Channel module (SFPs sold separately)   |                          |
| Services modules   | DS-X9308-SMIP   | 8-port Gigabit Ethernet IP storage services module.   |                          |
|                    | DS-X9032-SMV    | 32-port Fibre Channel Advanced Services Module (ASM).   |                          |
|                    | DS-X9560-SMC    | Caching Services Module (CSM)   |                          |

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

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

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

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

## Determining the Software Version



### Note

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

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

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

## Image Upgrade

The Cisco MDS SAN-OS software is designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

You can nondisruptively upgrade to (or downgrade from) Release 1.3(3c) using any Cisco MDS SAN-OS software release other than Release 1.0(2a).

## New Features in Release 1.3(3c)

Cisco MDS SAN-OS Release 1.3(3c) is a 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.



Note

The *Release Notes* are specific to this release. For the Cisco MDS SAN-OS Release 1.3 document set, see the “[Related Documentation](#)” section on page 17.



Caution

Cisco MDS SAN-OS Releases 1.3(2a) and 1.3(3) have been deferred. Please use Cisco MDS SAN-OS Release 1.3(3c) or later. Refer to [CSCee18613](#) for further information.

## Limitations and Restrictions

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

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

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

## Caveats

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

**Table 3** *Release Caveats and Caveats Corrected Reference*

| DDTS Number                | Software Release (Resolved or Open) |         |
|----------------------------|-------------------------------------|---------|
|                            | 1.3(3)                              | 1.3(3c) |
| <b>Severity 1</b>          |                                     |         |
| <a href="#">CSCed44067</a> | O                                   | O       |
| <a href="#">CSCee18613</a> | O                                   | R       |

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

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

| DDTS Number                | Software Release (Resolved or Open) |         |
|----------------------------|-------------------------------------|---------|
|                            | 1.3(3)                              | 1.3(3c) |
| <a href="#">CSCeg13762</a> | O                                   | O       |
| <b>Severity 2</b>          |                                     |         |
| <a href="#">CSCed35356</a> | O                                   | O       |
| <a href="#">CSCed42077</a> | O                                   | O       |
| <a href="#">CSCed57251</a> | O                                   | O       |
| <a href="#">CSCed65607</a> | O                                   | O       |
| <a href="#">CSCed75825</a> | O                                   | O       |
| <a href="#">CSCed88650</a> | O                                   | R       |
| <a href="#">CSCee01143</a> | O                                   | O       |
| <a href="#">CSCee06496</a> | O                                   | O       |
| <a href="#">CSCee22323</a> | O                                   | R       |
| <a href="#">CSCee43249</a> | O                                   | O       |
| <a href="#">CSCef83504</a> | O                                   | O       |
| <a href="#">CSCeg84871</a> | O                                   | O       |
| <a href="#">CSCei25319</a> | O                                   | O       |
| <a href="#">CSCsh27840</a> | O                                   | O       |
| <b>Severity 3</b>          |                                     |         |
| <a href="#">CSCea45726</a> | O                                   | O       |
| <a href="#">CSCea82028</a> | O                                   | O       |
| <a href="#">CSCec10009</a> | O                                   | O       |
| <a href="#">CSCec31365</a> | O                                   | O       |
| <a href="#">CSCed14360</a> | O                                   | O       |
| <a href="#">CSCed14920</a> | O                                   | O       |
| <a href="#">CSCed20053</a> | O                                   | O       |
| <a href="#">CSCed31611</a> | O                                   | O       |
| <a href="#">CSCed34922</a> | O                                   | O       |
| <a href="#">CSCed35965</a> | O                                   | O       |
| <a href="#">CSCed36114</a> | O                                   | R       |
| <a href="#">CSCed51574</a> |                                     | O       |
| <a href="#">CSCed58155</a> | O                                   | O       |
| <a href="#">CSCed63030</a> | O                                   | R       |
| <a href="#">CSCed64425</a> | O                                   | O       |
| <a href="#">CSCed93597</a> | O                                   | R       |
| <a href="#">CSCed94302</a> | O                                   | O       |
| <a href="#">CSCed96246</a> |                                     | O       |

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

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

| DDTS Number                | Software Release (Resolved or Open) |         |
|----------------------------|-------------------------------------|---------|
|                            | 1.3(3)                              | 1.3(3c) |
| <a href="#">CSCee04343</a> | O                                   | O       |
| <a href="#">CSCee54650</a> | O                                   | O       |
| <a href="#">CSCee89946</a> | O                                   | O       |
| <a href="#">CSCeg56197</a> | O                                   | O       |
| <a href="#">CSCeg61535</a> | O                                   | O       |
| <a href="#">CSCeg66225</a> | O                                   | O       |
| <a href="#">CSCeh21199</a> | O                                   | O       |
| <a href="#">CSCei91676</a> | O                                   | O       |
| <a href="#">CSCej08751</a> | O                                   | O       |
| <a href="#">CSCin81760</a> | O                                   | O       |
| <b>Severity 4</b>          |                                     |         |
| <a href="#">CSCeh42252</a> | O                                   | O       |

## Resolved Caveats

- [CSCee18613](#)

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

**Workaround:**

- This bug is fixed in Release 1.3(3c) and all subsequent releases.
- If you received the Cisco MDS Switch with a factory-installed SAN-OS Release1.3(x), you will not be affected by this bug.
- If you are currently running SAN-OS Releases 1.0(x), 1.1(x), or 1.2(x) and planning to upgrade to Releases 1.3(2a) or 1.3(3), be sure to schedule a switch reload after the SAN-OS upgrade.

- [CSCed88650](#)

**Symptom:** A malformed ELS frame destined to the RSCN process results in the packet not being discarded. This prevents RSCN process from receiving any further frames.

**Workaround:** None.

- [CSCee22323](#)

**Symptom:** After doing a VSAN delete operation, if a switchover or code upgrade is performed then FSPF will loose all the routes on all the higher numbered (than the VSAN that has been deleted) VSANs. As an example, if you have VSANs 1, 2 and 3 and now you delete VSAN 2, then you will see the FSPF routes missing in VSAN 3, after switchover/upgrade.

**Workaround:** Deleting and readding the affected VSANs or disabling and enabling FSPF on the VSANs will bring back the routes.

- [CSCed36114](#)

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

**Symptom:** Configuring the iSCSI TCP minimum bandwidth sets the maximum bandwidth; configuring the maximum bandwidth sets the minimum bandwidth.

**Workaround:** None.

- CSCed63030

**Symptom:** If Write Acceleration was enabled in some cases, the first few Fibre Channel data frames of an IO were not sent to the target for a FCIP write IO operation. This caused the IO operation to abort with a check-condition and also reset the connection to the initiator. This problem was caused by the FCIP Write Acceleration functionality which uses internal timers to free up resources. The software erroneously freed up buffered frames of pending write IO operations.

**Workaround:** None.

- CSCed93597

**Symptom:** The SAN-OS software rejects FDISC frames for the following cases:

- AIX Version 5.1 sends FDISC frame with all zeros. This is not allowed by the FC-FS standards.
- AIX Version 5.2 (without patch IBM APAR IY54881) has same issue as Case a (above), and sends the FDISC frame to FFFFFC instead of FFFFFE which is not allowed by the standards.
- The SAN-OS software did not handle the FDISC ELS command which displays N port ID, port WWN, and node WWN values obtained from a prior FLOGI session, but fills in zeros for the common service parameters.

**Workaround:**

- Irrespective of AIX fixes, the SAN-OS workaround is required to handle Case c (above).
- Even if Case a (above) is an AIX 5.1 issue, the SAN-OS patch allows Cisco MDS switches to work with existing AIX 5.1 installations.
- AIX Version 5.2 with patch IBM APAR IY54881 along with this SAN-OS patch addresses Case b (above).
- AIX Version 5.2 without the SAN-OS patch will not work as it sends FDISC to FFFFFC, for which no patch is intended in SAN-OS software.

## Open Caveats

- CSCed44067

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

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

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

- CSCeg13762

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

**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).

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

- CSCed35356

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

**Workaround:** None.

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

- CSCed42077

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

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

- CSCed57251

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

**Workaround:** None.

- CSCed65607

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

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

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

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

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

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

- CSCed75825

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

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

- CSCee01143

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

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

SNMP NotInTimeWindow

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

```
MDS# clock set 04:23:01 26 March 2000
MDS# clock set 04:23:01 11 November 2004
```

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

- CSCee06496

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

- Removing an IPS-8 module from the switch.
- Inserting a different type of module in the same slot.
- Configuring the new module.
- Issuing the **copy running-config startup-config** command.

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

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

- CSCee43249

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

**Workaround:** None.

- CSCef83504

**Symptom:** The system does not recognize a CLI password containing the “\$” character.

**Workaround:** Change your password to a different string that does not include the “\$” character. For an admin user-account, you might have to perform the password-recovery procedure to reset the password.

- CSCeg84871

**Symptom:** When an iSCSI initiator logs in to a Gigabit Ethernet port number 1 on an IPS module in slot 1, the switch sends a login response with the value of the Target Session Identifying Handle (TSIH) field set to zero (0), which is an iSCSI protocol violation. This situation can also occur when an iSCSI initiator logs in to Ethernet PortChannel number 1. The Qlogic iSCSI initiator may verify the TSIH value and reject it.

**Workaround:** None.

- CSCei25319

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

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

- CSCsh27840

**Symptom:** While using an FCIP link for remote SPAN, it is possible that the FCIP link may flap.

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

**Workaround:** Do not use FCIP links for Remote SPAN.

- CSCea45726

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

**Workaround:** None.

- CSCea82028

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

**Workaround:** Close the Device Manager and reopen it.

- CSCec10009

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

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

- CSCec31365

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

**Workaround:** None.

- CSCed14360

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

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

- CSCed14920

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

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

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

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

- CSCed20053

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

**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 run st** command. The **install license** command should work properly after that.

- CSCed31611

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

**Workaround:** None.

- CSCed34922

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

**Workaround:** None.

- CSCed35965

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

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

- CSCed51574

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

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

- CSCed58155

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

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

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

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

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

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

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

- CSCed64425

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

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

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

- CSCed94302

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

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

- CSCed96246

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

**Workaround:** Refer to the following URL for further information:

[http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod\\_technical\\_reference09186a008020fd0e.html](http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_technical_reference09186a008020fd0e.html)

- CSCee04343

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

**Workaround:** None.

- CSCee54650

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

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

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

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

- CSCee89946

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

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

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

```
switch# config t
switch(config)# interface fc2/1
switch(config)# shutdown
switch(config)# no shutdown
```

Issue the following commands to verify the module uptime.

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

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

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

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

Other notes:

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

- 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.

---

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

- CSCeh21199
 

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

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

**Workaround:** Upgrade to Cisco MDS SAN-OS Release 2.0(4).
- CSCei91676
 

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

**Workaround:** Limit the number of configured LUN maps for an iSCSI virtual target to fewer than 50 LUNs.
- CSCej08751
 

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

**Workaround:** None.
- CSCin81760
 

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

**Workaround:** None. Enable the license features again.
- CSCeh42252
 

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

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

## Related Documentation

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

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9100 Series Quick Start Guide*
- *Cisco MDS 9500 Series and Cisco MDS 9216 Switch Quick Start Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9000 Family Configuration Guide*

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

- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Fabric and Device Manager User Guide*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family System Messages Guide*
- *Cisco MDS 9000 Family MIB Reference Guide*
- *Cisco MDS 9000 Family CIM Programming Reference Guide*

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

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

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

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

## Obtaining Documentation

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

### Cisco.com

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

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

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

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](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

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

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

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

## Documentation Feedback

You can send comments about technical documentation to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).

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

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

We appreciate your comments.

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

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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](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](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



Tip

---

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

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

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

---

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

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

## Obtaining Technical Assistance

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

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

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

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

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

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

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

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

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

---

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



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