**Send documentation comments to mdsfeedback-doc@cisco.com**

# Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.0(4)

**Release Date: March 3, 2005**

**Text Part Number: OL-6249-04 W0**

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 19.

**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 | 03/03/2005 | Created release notes |
| B0 | 03/15/2005 | Added DDTS CSCed20053. |
| C0 | 04/12/2005 | Removed DDTS CSCeg07339<br>Added DDTS CSCeh49026, CSCeh44216, CSCeh48138, CSCeh51924 |
| D0 | 04/13/2005 | Added DDTS CSCeg81089 |
| E0 | 05/03/2005 | Added DDTS CSCeg82721 and CSCeh65824 |
| F0 | 05/19/2005 | Removed DDTS CSCeh44216 |
| G0 | 5/24/2005 | Added DDTS CSCeg66225 and CSCeh42252 |
| H0 | 5/31/2005 | Added DDTS CSCeh96928 |
| I0 | 06/01/2005 | Added DDTS CSCeg24199 |
| J0 | 06/23/2005 | Added DDTS CSCei25319 |

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

*Table 1 On-Line History Change*

| Revision | Date | Description |
|---|---|---|
| K0 | 08/04/2005 | Added DDTS CSCed57251, CSCeh61610, CSCeh64080, CSCec31365, CSCeg20932, CSCeg53114, CSCeg66225, CSCeh19639, CSCeh52280, CSCeh56143, CSCeh82490, CSCeh83514, CSCeh87985, CSCeg90336, CSCeh52973, CSCeh87930, CSCeh90270, CSCeh93625, CSCei01431, CSCeh73101, and CSCei29086 |
| L0 | 08/05/2005 | Added DDTS CSCeh41099 |
| M0 | 08/22/2005 | Removed DDTS CSCeh61610 |
| N0 | 08/23/2005 | Added DDTS CSCeh61610 |
| O0 | 12/07/2005 | Added DDTS CSCsc31424 |
| P0 | 12/30/2005 | Added DDTS CSCei91968 |
| Q0 | 05/03/2006 | Removed DDTS CSCeh52973<br>Added DDTS CSCeg33121, CSCsd29338, CSCei57342, CSCei58652, CSCei67982, CSCei91676, CSCsc09732, CSCsc33788, and CSCsd83775 |
| R0 | 06/06/2006 | Removed DDTS CSCed16845 |
| S0 | 09/05/2006 | Added DDTS CSCsd78967 |
| T0 | 09/13/2006 | Added DDTS CSCsf21970 |
| UO | 11/07/2006 | Added DDTS CSCsg15392 |
| V0 | 02/23/2007 | Added DDTS CSCse99087, CSCsg03171, and CSCsh27840. |
| W0 | 08/28/2007 | Modified the description of CSCsd83775. |

# Contents

This document includes the following sections:

# Introduction

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(4) and includes the following topics:


- Components Supported, page 3
- Determining the Software Version, page 6


## 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 | Not orderable | MDS 9500 Supervisor/Fabric-I, SAN-OS software. | MDS 9500 Series only |
| | Not orderable | MDS 9216 Supervisor/Fabric-I, SAN-OS software. | MDS 9200 Series only |
| | Not orderable | 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 | M9500ENT1K9 | Enterprise package. | MDS 9500 Series |
| | M9200ENT1K9 | Enterprise package. | MDS 9200 Series |
| | M9100ENT1K9 | Enterprise package. | MDS 9100 Series |
| | M9500FIC1K9 | Mainframe package. | MDS 9500 Series |
| | M9200FIC1K9 | Mainframe package. | MDS 9200 Series |
| | M9100FIC1K9 | Mainframe package. | MDS 9100 Series |
| | M9500FMS1K9 | Fabric Manager Server package. | MDS 9500 Series |
| | M9200FMS1K9 | Fabric Manager Server package. | MDS 9200 Series |
| | M9100FMS1K9 | Fabric Manager Server package. | MDS 9100 Series |
| | M9500EXT1K9 | SAN Extension over IP package for IPS-8 module. | MDS 9500 Series |
| | M9200EXT1K9 | SAN Extension over IP package for IPS-8 module. | MDS 9200 Series |
| | M9500EXT14K9 | SAN Extension over IP package for IPS-4 module. | MDS 9500 Series |
| | M9200EXT14K9 | SAN Extension over IP package for IPS-4 module. | MDS 9200 Series |
| | M9500EXT12K9 | SAN Extension over IP package for MPS 14+2 module. | MDS 9500 Series |
| | M9200EXT12K9 | SAN Extension over IP package for MPS 14+2 module. | MDS 9200 Series |
| | M9500SSE1K9 | Storage Services Enabler package. | MDS 9500 series with ASM or SSM |
| | M9200SSE1K9 | Storage Services Enabler package. | MDS 9200 series with ASM or SSM |
| 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[1] 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 |

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

| Component | Part Number | Description | Applicable Product |
|---|---|---|---|
| Supervisor modules | DS-X9530-SF1-K9 | MDS 9500 Supervisor/Fabric-I, module. | MDS 9500 Series only |
| Switching modules | DS-X9016 | MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately). | MDS 9500 Series and 9200 Series |
| | DS-X9032 | MDS 9000 32-port 1-Gbps/2-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-X9032-SSM | MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM). | |
| | DS-X9560-SMC | Caching Services Module (CSM). | |
| | DS-X9302-14K9 | 14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module. | |
| LC-type fiber-optic SFP | DS-SFP-FC-2G-SW | 2-Gbps/1-Gbps Fibre Channel — short wavelength SFP. | MDS 9000 Family |
| | DS-SFP-FC-2G-LW | 2-Gbps/1-Gbps Fibre Channel — long wavelength SFP. | |
| | DS-SFP-FCGE-SW | 1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP. | |
| | DS-SFP-FCGE-LW | 1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel — long wavelength SFP. | |
| CWDM[2] | CWDM-SFP-xxxx-2G | Gigabit Ethernet and 1-Gbps/2-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(4) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of the SAN-OS, upgrade to Release 1.3(x) and then Release 2.0(4).

When downgrading from Cisco MDS SAN-OS Release 2.0(4) to Release 1.3(x), you might need to disable new features in Release 2.0(4) for a nondisruptive downgrade. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade enables the compatibility check. The check indicates that the downgrade is disruptive and the reason is "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 MDS 9000 Family Configuration Guide* for more details.

# New Features in Cisco MDS SAN-OS Release 2.0(4)

**Note**

# Limitations and Restrictions

# Caveats

*Table 3 Release Caveats and Caveats Corrected Reference*

| | Software Release (Open or Resolved) | |
|---|---|---|
| **DDTS Number** | **2.0(3)** | **2.0(4)** |
| **Severity 1** | | |
| | | |
| | | |
| **Severity 2** | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

| DDTS Number | Software Release (Open or Resolved) | |
|---|---|---|
| | 2.0(3) | 2.0(4) |
| | | |
| **Severity 3** | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

| DDTS Number | Software Release (Open or Resolved) | |
|---|---|---|
| | 2.0(3) | 2.0(4) |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Severity 4** | | |
| | | |

# Resolved Caveats

- **Symptom**

  **Workaround**

# Open Caveats

- **Symptom** **show running-config** **show startup-config** **copy running-config startup-config**

  **Workaround**

- **Symptom**

**Workaround**

- **Symptom**

  **copy running-config startup**

  **Workaround**

- **Symptom**

  **Workaround** **Admin > Fabrics**

- **Symptom:**

  **Workaround:**

- **Symptom**

  **Workaround**

- **Symptom**

  **install all**

- **Symptom**

  **Workaround**
  than 25 Mega bits/sec. There is no workaround if the throughput requirement is > 25 Mbps.

- CSCeg90336

  **Symptom**: A user that you create in Fabric Manager or Device Manager cannot log in from the console. Release 2.1(2) fixes this problem. However, if a third-party application creates a user using SNMP, a new MIB is required for Release 3.0.

  **Workaround**: Third-party applications should use SSH to connect to the MDS 9000 switch, and then use CLI commands to create the user account.

- 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.

- CSCeh87930

  **Symptom**: A newly configured FCIP link may fail to come up when running on an MPS-14/2 module. This symptom may occur following an upgrade of Cisco MDS SAN-OS Release 2.0(1b) to Release 2.0(3) and the configuration of a new FCIP link.

  In the log on the switch, you may see the following messages:

  ```
  %PORT-5-IF_DOWN_ELP_FAILURE_ISOLATION: %$VSAN xyz%$ Interface fcipabc is down
  (Isolation due to ELP failure)
  %PORT-5-IF_DOWN_OFFLINE: %$VSAN xyz%$ Interface fcipabc is down (Offline)
  %PORT-5-IF_DOWN_NONE: %$VSAN xyz%$ Interface fcipabc is down (None)
  ```

  VSAN xyz is the allowed VSAN number for the FCIP interface and interface fcipabc is the configured FCIP interface number.

  : Reload the MPS-14/2 module using the ***module-number*** command, where ***module-number*** is a specific module.

- CSCeh90270

  : Two MDS 9000 switches configured with an FCIP bridge port (B port) tunnel may have problems with multi-frame sequences. You may notice this problem activating large zone sets when the SFC frame times out.

  : If the connection is between two MDS switches, then the B port configuration is not required and should not be used. If B port is a requirement, then reduce the zone set length by not distributing the full database, or useVSANs.

- CSCeh93625

  : The modules shut down after the supervisor module fails.

  : Remove the failed supervisor module and reinsert the line card. Or enter the ***slot*** command in Exec mode on the switch, where ***slot*** is the slot number of the module that failed.

- CSCeh96928

  : 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.

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

- CSCei01431

  : An FCIP interface stays in the initializing state if it is part of a PortChannel and it is removed with the command.

  : Remove the PortChannel that the FCIP interface previously belonged to.

- CSCei25319

  : 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.

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

- CSCsd78967

  : 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.

  : None.

- CSCsh27840

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

  : Do not use FCIP links for Remote SPAN.

- CSCec31365

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

  : None.

- CSCed14920

  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 command at the prompt—the command output displays the following information:

  –

  –

  *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

- *remote-url*

- *application_name*

- 
- 
- 
- 
- 
- 
- 
- 
  a. 
  b. 
  c. 
  d. 
  e. 

f. **Ctrl-z**

**Workaround**

- 

**Symptom**
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.

- 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

- 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).
```

**Workaround**

**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 LINIT requests.

**Workaround**

**Symptom**

**Workaround**

**Symptom**

**Workaround**

**Symptom**

**Workaround**

**Symptom**

**Workaround**

**Symptom** **copy *<config-url>* startup**

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

: Issue the command from the switchboot prompt.

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

CSCeg61535

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

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

CSCeh73101

: When you perform a nondisruptive upgrade from Release 1.3(x) to 2.0(x), and then issue the command, the switch displays the wrong user. The user shown will be inconsistent with the user shown when you issue the command.

: Recreate the user.

CSCeg81089

: 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".

: 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

: The command output shows the callhome profile alertgroups with an underscore ( _ ) rather than a dash ( - ). If the 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.x code and cannot be deleted. This occurs if the following alert groups have been configured:

cisco_tac

supervisor_hardware

linecard_hardware

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

cisco_tac

supervisor_hardware

linecard_hardware

CSCeh82490

: 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.

: None.

CSCeh83514

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

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

CSCeh87985

: When no role is associated with a user, SNMP fails when the 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.

: Associate at least one role (group) to the user by executing the [ ] command in configuration mode.

CSCei29086

: Following the installation of a third-party syslog server to a PC running Fabric Manager and Device Manager, the third-party syslog server takes ownership of the PC's IP address as the syslog server. As a result, the MDS switch is no longer able to act as the syslog server.

You can see the error message "java.lang.NullPointerException" if you verify syslog on the MDS switch through Device Manager by choosing **Logs > Syslog > Verify**.

If you uninstall the third-party software and verify syslog again with **Logs > Syslog > Verify**, you see the error message "Can't connect to FM server."

**Workaround**: To allow the MDS 9000 switch to be the syslog server, follow these steps:

1.
2. **My Computer > Manage > Services and Applications > Services**
3.

- **Symptom**

  **Workaround** **shut** **no shut**

- **Symptom**

  **Workaround**

- **Symptom**

  **Workaround**

- **Symptom**

  **Workaround**

- **Symptom**

  **Workaround**

- **Symptom**
  **show running** **show startup**
  **show boot**

  **Workaround** **show boot**

-

**Symptom**

**show**

**Workaround**

- **Symptom** **no shutdown**

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

**Workaround** **channel-group X**
**no interface port-channel X**
**no shutdown**

- **Symptom** **install all**

```
%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
```

**install all**

**Workaround**

- **install module** *module-number* **image**
**reload module** *module-number* **force-dnld**

**Symptom**

**Workaround** **fcdomain restart vsan** *vsan-id*

**Symptom**

```
SNMP: Unknown username
```

**Workaround**

**Symptom**

**Workaround**

**Symptom**

**Workaround**

**Symptom**

**Workaround** **shutdown**

**no shutdown**

**Symptom**

**Workaround**

*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*

*Cisco MDS SAN-OS Compatibility Matrix for Storage Service Interface Images*

*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 and Downgrade 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 bug-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. through 8. .

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/

- 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

- 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

- 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.