Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.3(6)

Release Date: November 5, 2004

Text Part Number: OL-4959-08, R0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with the documents listed in the "Related Documentation" section on page 11.

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

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

Table 1 On-Line History Change

Revision	Date	Description
A0	11/05/2004	Release note created.
B0	11/05/2004	Removed the following resolved caveats: CSCee51071, CSCee89946, CSCef04575, CSCef06657, CSCee95629, CSCin74613, CSCee04343, CSCee28076, CSCee34199, CSCee38287, CSCed64425, CSCef12062, CSCee79377, CSCee65091, CSCee54650, CSCef21105, CSCee83961
C0	11/09/2004	Added SSE license information.
D0	11/17/2004	Added DDTS CSCeg23889 and image upgrade references.
E0	12/07/2004	Added DDTS CSCef65409
F0	12/08/2004	Added DDTS CSCin81760
G0	12/22/2004	Added DDTS CSCeg61535
H0	01/14/2005	Added DDTS CSCeg56197.
I0	02/17/2005	Corrected the state of DDTS CSCef83504

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

Table 1 On-Line History Change (continued)

Revision	Date	Description
J0	03/24/2005	Added DDTS CSCed20053, CSCeh21199. Removed DDTS CSCee26227. Resolved in previous release.
K0	05/31/2005	Added DDTS CSCeh42252 and CSCeg66225.
L0	06/23/2005	Added DDTS CSCei25319.
M0	07/29/2005	Added DDTS CSCed57251, CSCeh61610, CSCeh64080, and CSCec31365.
N0	08/22/2005	Removed DDTS CSCeh61610.
O0	08/23/2005	Added DDTS CSCeh61610.
P0	05/01/2006	Added DDTS CSCeg33121, CSCeg84871, CSCei91676, CSCej08751, and CSCsc33788.
Q0	06/06/2006	Removed DDTS CSCed16845.
R0	02/26/2007	Added DDTS CSCsh27840.

Contents

This document includes the following sections:

Introduction

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

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

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 1.3(6) and includes the following topics:

Software and Hardware 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 Products
Software	M95S1K9-1.3.6	MDS 9500 Supervisor/Fabric-I SAN-OS software	MDS 9500 Series only
	M92S1K9-1.3.6	MDS 9216 Supervisor/Fabric-I SAN-OS software	MDS 9216 only
	M91S1K9-1.3.6	MDS 9100 Supervisor/Fabric-I SAN-OS software	MDS 9100 Series only
License	M9500SSE1K9	Storage services enabler package	MDS 9500 series with ASM
	M9500SSE1K9	Storage services enabler package	MDS 9200 series with ASM

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

Component	Part Number	Description	Applicable Products
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately)	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately)	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16-port 1 Gbps/2Gbps 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-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 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9216
	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-X9560-SMC	Caching Services Module (CSM)	
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	1-Gbps/2-Gbps Fibre Channel — short wavelength SFP	MDS 9000 Family
	DS-SFP-FC-2G-LW	1-Gbps/2-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	

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

Component	Part Number	Description	Applicable Products
CWDM[2]	DS-CWDM-1470	1470 NM CWDM GE and 2-Gbps FC SFP	MDS 9000 Family
	DS-CWDM-1490	1490 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1510	1510 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1530	1530 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1550	1550 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1570	1570 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1590	1590 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-1610	1610 NM CWDM GE and 2-Gbps FC SFP	
	DS-CWDM-MUX-4	Add/drop multiplexer for 4 CWDM wavelengths	
	DS-CWDM-MUX-8	Add/drop multiplexer for 8 CWDM wavelengths	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexer(s)	
Power supplies	DS-CAC-300W	300-W AC power supply	MDS 9100 Series only
	DS-CAC-845W	845-W[3] AC power supply	MDS 9216 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, 512 MB	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 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 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 SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, from the Switches tab in the information pane, locate the switch using its IP address, logical name, or WWN, and then 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 (or downgrade from) Release1.3(6) using any Cisco MDS SAN-OS software release other than Release 1.0(2a).

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

New Features

There are no new features for this release.

Caveats

This section lists the open and resolved 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 Open and Resolved Caveats by Severity

DDTS Number	Software Release (Resolved or Open)	
	1.3(5)	1.3(6)
Severity 1		
CSCeg13762	O	R
CSCeg33121	O	O
Severity 2		
CSCed57251	O	O
CSCef65409	O	R
CSCef83504	O	O
CSCeg18886	O	R
CSCeg23889	O	O
CSCeg84871	O	O
CSCeh61610	O	O
CSCei25319	O	O
CSCsh27840	O	O

Table 3 Open and Resolved Caveats by Severity (continued)

DDTS Number	Software Release (Resolved or Open)	
	1.3(5)	1.3(6)
Severity 3		
CSCec31365	O	O
CSCed14920	O	O
CSCed20053	O	O
CSCef70000	O	O
CSCeg56197	O	O
CSCeg61535	O	O
CSCeg66225	O	O
CSCeh21199	O	O
CSCeh64080	O	O
CSCei91676	O	O
CSCej08751	O	O
CSCin81760	O	O
CSCsc33788	O	O
Severity 4		
CSCeh42252	O	O

Resolved Caveats

- 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).

- CSCef65409

  Symptom: SNMP daemon crashes periodically on a Cisco MDS 9000 Family switch running Release 1.3(4a). Issue the **show process memory | include snmp** commands at regular intervals to show the pattern of a memory increase.

  Workaround: Upgrade to Cisco MDS SAN OS Release 1.3(6).

- CSCeg18886

  Symptom: If multiple “get all next” queries are sent before receiving a response from the first one, some queries might be dropped as they overwhelm the name server buffers. Some arrays do this to improve performance, resulting in dropped queries.

  Workaround: Upgrade to Cisco MDS SAN-OS Release 1.3(6).

Open Caveats

- CSCeg33121

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

  Workaround: None.

- CSCed57251

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

  Workaround: None.

- 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.

- CSCeg23889

  Symptom: License warning notifications, either through Call Home or system messages, might occur in the following situations:

  - The grace period for a license package was triggered (a feature licensed by that license package had been used). Currently none of the features licensed by this license package are enabled.
  - The grace period for a license package expired. None of the features licensed by this license package are enabled.

  Workaround: None.

- 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.

- CSCeh61610

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

  Workaround: None.

- CSCei25319

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

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

- CSCsh27840

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

Workaround: Do not use FCIP links for Remote SPAN.

- CSCec31365

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

  Workaround: None.

- CSCed14920

  Symptom: During a switch upgrade, a SAN Volume Controller (SVC) node may not save its entire state under rare circumstances. After the switch upgrades, the node is not part of the cluster. Verify this symptom by issuing the **show nodes local** command at the `svc-config` prompt—the command output displays the following information:

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

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

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

- CSCed20053

  Symptom: On rare occasions, the **install license** command may fail due to the saved state of the switch configuration. This may occur after saving a remote configuration to the switch using the **copy** *remote-url* **start-up** command.

  Workaround: Issue the **copy ru st** command. The **install license** command should work properly after that.

- CSCef70000

  Symptom: If you downgrade from Cisco MDS SAN-OS Release 1.3(5) to Release 1.3(4), then you might lose your per-VSAN in-order delivery configuration.

  Workaround: Reconfigure your system with the per-VSAN in-order delivery configuration.

- 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.

- 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).

- CSCeh64080

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

  Workaround: None.

- 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.

- CSCsc33788

  Symptom: In rare circumstances, after you issue the **install all** command to upgrade an MDS switch, the upgrade may fail because the installer process fails. When this occurs, you may see a message like the following:

  ```
  %CALLHOME-2-EVENT: SW_CRASH alert for service: installer
  The installer failed to respond for 10 times. Exiting ...
  Unable to send exit to installer. Return code -1
  ```

If you upgrade from 1.3(x) to 2.1 or from 2.0(x) to 2.1 and the upgrade fails, and if after the upgrade failure the supervisor modules are running the new software version, but some modules are running the older software version, then the next attempt to execute the **install all** command will trigger this problem.

You should not encounter this problem if you upgrade from 2.1 to a higher version.

Workaround: There are two ways to address this issue:

- To non-disruptively upgrade all modules that are running the older software version, issue the **install module** *module-number* **image** command.
- To disruptively upgrade the modules, issue the **reload module** *module-number* **force-dnld** command, or reinstall the module.

- CSCeh42252

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

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

Related Documentation

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

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

- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: http://support.veritas.com/

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website: http://www.ibm.com/storage/support/2062-2300/

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

You can send comments about technical documentation to mdsfeedback-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

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