Release Notes for TopspinOS Release 2.9.0

Release Date: November 6, 2006
Part Number: OL-9388-04

Contents

This document contains these sections:

Introduction

These release notes describe the features and known issues for the Topspin and Cisco SFS Series Product Family operating system 2.9.0 FCS (build 147) and Element Manager 2.9.0.8 software releases.

Note These release notes apply to the Topspin 120, Topspin 270, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 7000P, Cisco SFS 7008P, and Cisco SFS 7000D switches that run TopspinOS 2.9.0 software.

Cisco Systems

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

System Requirements

This section describes the system requirements for this software release.

Determining the Software Version

To determine the version of the operating system that you are running on the switch, log in to the CLI and enter the **show version** EXEC command.

```
SFS-7000P> show version
=========================================================================
                           System Version Information
=========================================================================
system-version : TopspinOS 2.9.0 releng #147 …
contact : tac@cisco.com
name : SFS-7000P
```

Upgrading to a New Software Release

To verify that you are running the latest available release, compare your version against the latest version on the Cisco support website at http://www.cisco.com/cgi-bin/tablebuild.pl/sfs-7000. After registering your product, you should have received a username and password that grant you access to this site.

Switch software and Linux host drivers are now released and packaged separately. Switch software is also now packaged and released separately for the following products:

- Cisco SFS 7000, 7000P, 7000D, 7008, and 7008P chassis—2.9.0 FCS
- Topspin 120 and 270 chassis—2.9.0 FCS
- 4X InfiniBand Switch Module for IBM BladeCenter H—2.6.0 FCS
- 1X InfiniBand Switch Module for IBM BladeCenter—2.6.0 FCS
- Cisco SFS 3001 and 3012 I/O chassis—2.4.0 Update 1
- Topspin 90 and 360 I/O chassis—2.4.0 Update 1

The TopspinOS 2.9.0 release supports 3.0.0 (or higher) Linux host drivers. The 3.0.0 Linux host drivers require that all switches first be upgraded to TopspinOS 2.1.0 or higher.

Old and new TopspinOS releases can be used in the same InfiniBand fabric, although InfiniBand subnet manager synchronization will not occur between TopspinOS 2.9.0 and older releases.

Switches should be upgraded before the InfiniBand hosts. The CLI **install** command will prevent an incompatible software image from being installed. To upgrade Element Manager (EM) GUI, first uninstall the older version and then install software release 2.9.0.

For general information about upgrading to a new software release, see the Install Software Images section in the *Cisco SFS 7000 Series Product Family Chassis Manager User Guide.*

New and Changed Information

TopspinOS 2.9.0 is a major release that introduces significant new features and documentation. It includes the following changes:

- Support for SFS 7000D InfiniBand switch

- Full configuration and management of 20 Gbps InfiniBand Double Data Rate links
- Ability to disable IPoIB on an InfiniBand partition for improved security
- Improved syslog and CLI compatibility with other Cisco products
- Ability to route around InfiniBand components that need maintenance
- Many bug fixes

Changes From Release 2.7.0 FCS (build 14) to 2.9.0 FCS (build 147)

This section describes the new features and resolved caveats since the 2.7.0 FCS (build 14) release.

Note The ID number from the Cisco Defect Tracking System, if applicable, is included with this format: CSCxxyyyyy. The current status of all issues is available online at http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. Contact Cisco Technical Support for more information.

InfiniBand

- CSCse96660, CSCse52949

  Support has been added for configuration and management of 20 Gbps InfiniBand Double Data Rate links. All CLI, SNMP, and GUI areas support DDR. Note that the longest DDR copper IB cable supported at this time is 8 meters.

- CSCse95216

  Support has been added for disabling IPoIB on an InfiniBand partition. This feature can be used to increase security on the default IB partition FFFF. Note that in 2.9.0 the mgmt-ib management InfiniBand interface cannot be used with a non-default IB partition.

- CSCsd83004

  Support has been added for routing around InfiniBand components that need maintenance. This feature adds a new **route-around** IB CLI command that isolates the component without disrupting traffic.

- CSCse38656

  Support has been added for automatically determining the maximum number of hops (depth) that the InfiniBand subnet manager has to search when configuring the InfiniBand fabric. This feature adds a new value 0 to the **max-hops** IB CLI configure command, which will cause the Subnet Manager to optimize IB paths for shortest distance.

Management

- CSCse39952

  TopspinOS 2.9.0 is the first release to support the SFS 7000D chassis. The management Ethernet port on the 7000D defaults to using DHCP to obtain an IP address.

- CSCtp01063

  Support has been added for clearing InfiniBand switch port counters with the new **clear** CLI command.

- CSCse39550

  A problem has been fixed where CLI SSH logins would not authenticate with RADIUS or TACACS+.
- CSCse38550

  A problem has been fixed where CLI logins would authenticate using local passwords after RADIUS or TACACS+ authentication failed.
- CSCse54928

  Syslog message format is now more consistent with other Cisco products.
- CSCse88972, CSCsf24942, CSCtp01362

  CLI error handling for incorrect commands is now more consistent with other Cisco products.
- CSCsg31514

  A problem has been fixed where command editing did not work properly in CLI SSH logins.
- CSCse36832

  A problem has been fixed where the CLI **copy** command would fail with symbolic links on a remote FTP server.
- CSCtp06939

  A problem has been fixed where the CLI **copy** command would fail with filenames longer than 128 characters.
- CSCtp06599, CSCtp06538, CSCsg15998

  Several problems were fixed in the CLI diagnostic test commands.

Changes From Release 2.5.0 Update 1 (build 251) to 2.7.0 FCS (build 14)

This section describes the new features and resolved caveats since the 2.5.0 Update 1 (build 251) release.

InfiniBand

- CSCsd86736, CSCsd56088, CSCse18870

  On SFS 7000P and SFS 7008P, power to an InfiniBand-powered interface is now turned off when the port is shut down. Power status is now displayed along with other port status values.
- CSCsd57775

  Added support for viewing the InfiniBand Linear Forwarding Table (LFT) and Multicast Forwarding Table (MFT) to SNMP, Element Manager GUI, and CLI.
- CSCsd55622

  Added support for configuring several more InfiniBand Subnet Manager parameters.

Management

- CSCsd43751

  Added support for viewing Cisco-standard Unique Device Indentifier Information with the new **show inventory** CLI command.
- CSCsd57699

  Added support for authentication with TACACS+.
- CSCsd54558

  Added support for secondary syslog server.
- CSCsd73467

  Added support for up to three RADIUS servers.
- CSCsd89599

  Added support for displaying a CLI login banner through the optional **config:login-banner** file.
- CSCtp05680

  The **show card-inventory** CLI command now displays uptime (number of seconds since booting) for each card.
- CSCtp02078, CSCsd68686, CSCsd68674, CSCse00615, CSCse08205, CSCse08216

  Several problems were fixed in hardware fault error reporting.

Changes Since Software Release 2.5.0 FCS (build 241)

This section describes the new features and resolved caveats since the 2.5.0 FCS (build 241) release.

InfiniBand

- CSCsd10909

  Fixed a problem in which the sm-info information about other InfiniBand subnet managers could be incorrect after a fabric merge.
- CSCsd34069

  Fixed a problem in route calculation for heterogeneous InfiniBand fabrics that use a mixture of 1X, 4X, and 12X links.

Management

- CSCsd29798, CSCsd29835, CSCsd31190, CSCsd31289

  Fixed several problems in Chassis Manager Web GUI.
- CSCsd33064

  Fixed a problem in Element Manager GUI in which multiple diagnostic tests could not be run.
- CSCsd28296

  Fixed a problem in which Management Interface Module Power On Self-Test (POST) could incorrectly fail on Topspin 270 and Cisco SFS 7008.

Changes Since Software Release 2.3.0 FCS (build 222)

This section describes the new features and resolved caveats since the 2.3.0 FCS (build 222) release.

InfiniBand

- CSCtp04427, CSCtp06472

  InfiniBand packet lifetimes are now configurable.
- CSCtp06383

  An InfiniBand subnet manager crash under heavy load has been fixed.
- CSCsc46269

  The performance of the InfiniBand subnet manager has been improved.
- CSCsc49085

  The InfiniBand subnet manager now has improved route calculation for heterogeneous InfiniBand fabrics that use a mixture of 1X, 4X, and 12X links.
- CSCtp06908

  Support for viewing the other InfiniBand subnet managers in a subnet has been added to SNMP, Element Manager GUI, and the new **show ib sm sm-info** CLI command.
- CSCtp06909

  Support for viewing the InfiniBand event subscribers in a subnet has been added to SNMP, Element Manager GUI, and the new **show ib sm subscription** CLI command.
- CSCsc46206

  Support has been added for configuring the maximum number of hops (depth) that the InfiniBand subnet manager has to search when configuring the InfiniBand fabric. This feature can be used to increase Subnet Manager performance on large fabrics.

Management

- CSCsd05202

  A problem has been fixed that caused the management Ethernet port to stop working.
- CSCtp06503

  Support for secure copy (scp) has been added.
- CSCsc46894

  Support for Cisco Discovery Protocol (CDP) has been added.
- CSCtp06811

  Added additional SNMP traps for Power On Self-Test (POST) failures. The Topspin 120, Cisco SFS 7000, and Cisco SFS 7000P will also send SNMP traps for hardware failures detected during normal operation.
- CSCtp06588

  The Ethernet management port (interface mgmt-ethernet) on the Topspin 270 and Cisco SFS 7008 now supports DHCP.

- CSCtp05360

  Additional Real Time Clock (RTC) hardware fault handling support has been added on Cisco SFS 7000P, SFS 7000, and Topspin 120.
- CSCsc96864

  Fixed a problem where an ECC error was detected but not handled correctly, causing the switch to reboot.
- CSCtp04448

  Added additional SNMP traps for power supply up and fan up events.

Changes Since Software Release 2.2.0 Update 1 (build 545)

This section describes the new features and resolved caveats since the 2.2.0 update 1 (build545) release.

InfiniBand

- CSCtp06338

  Support for user-configurable InfiniBand multicast groups has been added.
- CSCtp06557

  A Performance Management (PM) memory leak has been fixed. This memory leak, which occurred over time when monitoring was enabled or port counters were retrieved many times, could exhaust system memory and cause a chassis reboot.
- CSCtp05974, CSCtp05942, CSCtp06400

  Fault handling support for InfiniBand internal link errors has been added for Topspin 270 and Cisco SFS 7008. Internal InfiniBand link failures cause the system LED and the LEDs on the two involved Fabric Modules to turn amber. The **show diag fru-error** command can be used to get more information on the failure.
- CSCtp05747

  The management InfiniBand interface now supports a nondefault InfiniBand subnet prefix.
- CSCtp06168

  A problem has been fixed that caused InfiniBand ports to go down on Topspin 270 and Cisco SFS 7008 after Fabric Module node cards were rebooted.
- CSCtp06358

  A problem has been fixed where a synchronized standby Subnet Manager shutting down could cause the master Subnet Manager to stall.
- CSCtp06312

  Several scenarios have been fixed where a master and standby Subnet Manager could get out of synchronization.

Management

- CSCtp06319

  Topspin 270 and Cisco SFS 7008 software upgrade issues involving two Fabric Module cores have been resolved. Symptoms included LEDs stuck on or blinking, the Management Interface Module in slot 16 that showed a card type as Unknown, and I2C errors on the Management Interface Module in slot 16.

- CSCtp05923

  The Topspin 270 and Cisco SFS 7008 LIM card self-test now detects VPD (Vital Program Data) corruption.

- CSCtp05653

  The diagnostic card **self test** command has been fixed to not run out of system resources if it is repeatedly started and stopped before the command has completed.

- The **show diag post** and **show diag fru-error** commands now report descriptive values for problems instead of integer error codes.

- CSCtp05815

  The **show diag post** and **show diag fru-error** commands now report the correct fan FRU numbers.

- CSCtp05922

  The **show diag post** command now displays errors detected on the Topspin 270 and Cisco SFS 7008 standby Management Interface Module.

- CSCtp05936

  The Topspin 270 and Cisco SFS 7008 fan test self-test now detects a dead fan.

- CSCtp05342

  Additional hardware fault handling support has been added for Topspin 120, including checking for ECC, I2C, and Summit.

- CSCtp06436

  Some Topspin 120 Ethernet management ports were not programmed with a unique MAC address. This problem has been fixed.

- CSCtp06440

  Some power supplies on Topspin 270 and Cisco SFS 7008 were programmed with the wrong FRU Number in the VPD. This is now detected and corrected.

- CSCtp06047

  It is now possible to upgrade software on the Topspin 270 and Cisco SFS 7008 standby core Fabric Module using an EM or Web GUI upgrade. Previously, only the CLI could be used to upgrade the standby core.

- CSCtp05965

  The Topspin 270 and Cisco SFS 7008 Fabric Module Power On Self-Test (POST) for Management Interface Modules now runs only from core cards. Previously, POST also ran on node cards too, which would result in false failure error messages in the log files on node cards.

- CSCtp05857

  A power supply self test was added for the Topspin 120.

- CSCtp05487

  It is now possible to shut down a power supply on Topspin 270 and Cisco SFS 7008.

Caveats

This section describes temporary limitations of this release. These restrictions will be resolved in a future release of this product.

InfiniBand

- CSCtp05858

  In autonegotiation mode, it is possible for an unconnected InfiniBand port to report errors if the port is part of a cluster of three ports, where at least one of the other ports is connected.

Management

- CSCsg27834

  On Windows Internet Explorer, the Chassis Manager web interface may pop up in front of all other windows while running. This condition is due to a bug in the Sun JVM and is fixed in the latest Sun release, which can be downloaded at http://www.java.com/en/download/windows_ie.jsp.

- CSCsg55840

  The InfiniBand subnet manager **max-hops** value cannot be set to 0 from CLI.

  Workaround: Use EM or Chassis Manager GUI instead.

- CSCsg55985

  An InfiniBand subnet manager **max-hops** value of 0 is not persistent across chassis reboots.

  Workaround: Set **max-hops** to 0 each time the chassis is rebooted.

- CSCtp06432

  The Topspin 270, Cisco SFS 7008, and Cisco SFS 7008P Management Interface Module firmware is not automatically upgraded on hotplug (hotswap). If a new Management Interface Module is inserted into the chassis, the chassis should be rebooted or power-cycled to ensure that the firmware is upgraded.

- CSCtp04462, CSCtp05567, CSCtp05620

  The **diagnostic interface ib** commands are not supported.

- CSCtp05299

  Diagnostic tests should not be run during a Topspin 270, Cisco SFS 7008, and Cisco SFS 7008P controller hot standby failover. The diagnostic commands should not be run until all cards are up and running.

- CSCtp05446

  If a power cycle is performed on a Topspin 270, Cisco SFS 7008, and Cisco SFS 7008P after a software upgrade, rather than performing a **reload** command, it is possible that the core fabric in slot 12 can become the master after the power cycle.

- CSCtp05816

  It is possible for POST to detect a fan that is not completely plugged in, but the error does not show up in the **show diag post** or **show diag fru-error** command output. The error is reported in the hwif_log.
- CSCtp04365

  The Topspin 270, Cisco SFS 7008, and Cisco SFS 7008P incorrectly attempts to boot when no Management Interface Modules are present.
- The output of the CLI **show power-supply** command will have blank Power-supply Seeprom fields for some Topspin 270, Cisco SFS 7008, and Cisco SFS 7008P power supplies.
- CSCtp00587

  The Ethernet management port (interface mgmt-ethernet) 100Base-T supports only full-duplex connectivity.
- CSCtp01801

  If a firmware upgrade fails, the CLI does not report why the failure occurred.

  Workaround: Use the **show logging end** command to review the failure.
- CSCtp02078

  The error messages in the **show logging** command for environmental monitoring failures, such as failed power supplies, are cryptic.
- CSCtp00813

  The CLI does not provide any diagnostics if the NTP server(s) is not responding.
- CSCtp01498

  After executing the CLI **delete** or **clock set** commands, the CLI **reload** command will unnecessarily prompt if you wish to save changes.
- CSCtp02196

  The EM GUI will not install if there is not sufficient temporary space in /tmp.
- CSCtp01285

  The Serial/Mgmt-Ethernet and Maintenance->System Info windows in the GUI may not display if the GUI has been running for a while.
- CSCtp01977

  The ALT-TAB icon for the Element Manager GUI is blank on Linux.

Related Documentation

The following list describes the documentation available with TopspinOS 2.9.0, which is available in electronic form and printed form upon request.

Note Documentation is included on the TopspinOS 2.9.0 Server Switch CD Image.

You can download the latest documentation updates on the Cisco support site at http://www.cisco.com/en/US/partner/products/ps6418/tsd_products_support_category_home.html.

- *InfiniBand Hardware Installation and Cabling Guide*

- *Cisco SFS 7000P Switch Installation and Configuration Note*
- *Cisco SFS 7000P Hardware Installation Guide*
- *Cisco SFS 7008P Switch Installation and Configuration Note*
- *Cisco SFS 7008P Hardware Installation Guide*
- *Release Notes for TopspinOS Release 2.9.0*
- *Cisco SFS 7000 Series Product Family Chassis Manager User Guide*
- *Cisco SFS 7000 Series Product Family Element Manager User Guide*
- *Cisco SFS 7000 Series Product Family Command Reference Guide*

Service and Support

For additional support, you must first register your product at http://www.cisco.com. After registering, you may contact your supplier for support, or Cisco directly.

Refer to the "Obtaining Technical Assistance" section on page 14 in this document.

When you call Cisco Technical Support or use the Cisco Technical Support website at http://www.cisco.com, be prepared to provide the following information to support personnel:

General Information

- Technical Support registration number, if applicable
- Error messages received
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results

Server Configuration

- Type of server, chip set, CPU, amount of RAM, and number of nodes
- Attached storage devices (output from cat /proc/scsi/scsi)
- InfiniBand configuration (output from /usr/local/topspin/sbin/hca_self_test)

Chassis Configuration

- Chassis model
- Output from the **show running-status all** command

Chassis Serial Number

The chassis serial number and corresponding bar code are provided on the serial number label, as shown in this example:

Model: TS360

SN UST323XXXXXXXXX

This chassis serial number can be found on the bottom of the chassis or the outside of the chassis box packaging. It can also be found in the output of the **show backplane** command.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

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

http://www.cisco.com/techsupport

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

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

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

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

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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 at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 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 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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.