Release Notes for Cisco BLISS for Cable Release 2.2.1

Revised: August 10, 2006, Version OL-10982-01

This document describes the Cisco Broadband Local Integrated Services Solution (BLISS) for Cable, Release 2.2.1.

Note These release notes are updated periodically on an as-needed basis. Always read the applicable sections in their entirety, because they contain important operational information that can impact your network.

Feature History

Document Number	Modification
OL-10982-01	First issue of this document.

Contents

The following sections provide information specific to Release 2.2.1 of the Cisco BLISS for Cable solution:

The following sections provide links to additional Cisco resources:

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

- Obtaining Additional Publications and Information, page 11

Documentation for Cisco BLISS for Cable, Release 2.2.1

This section provides links to the solution-level and component-level documentation, and includes the following sections:

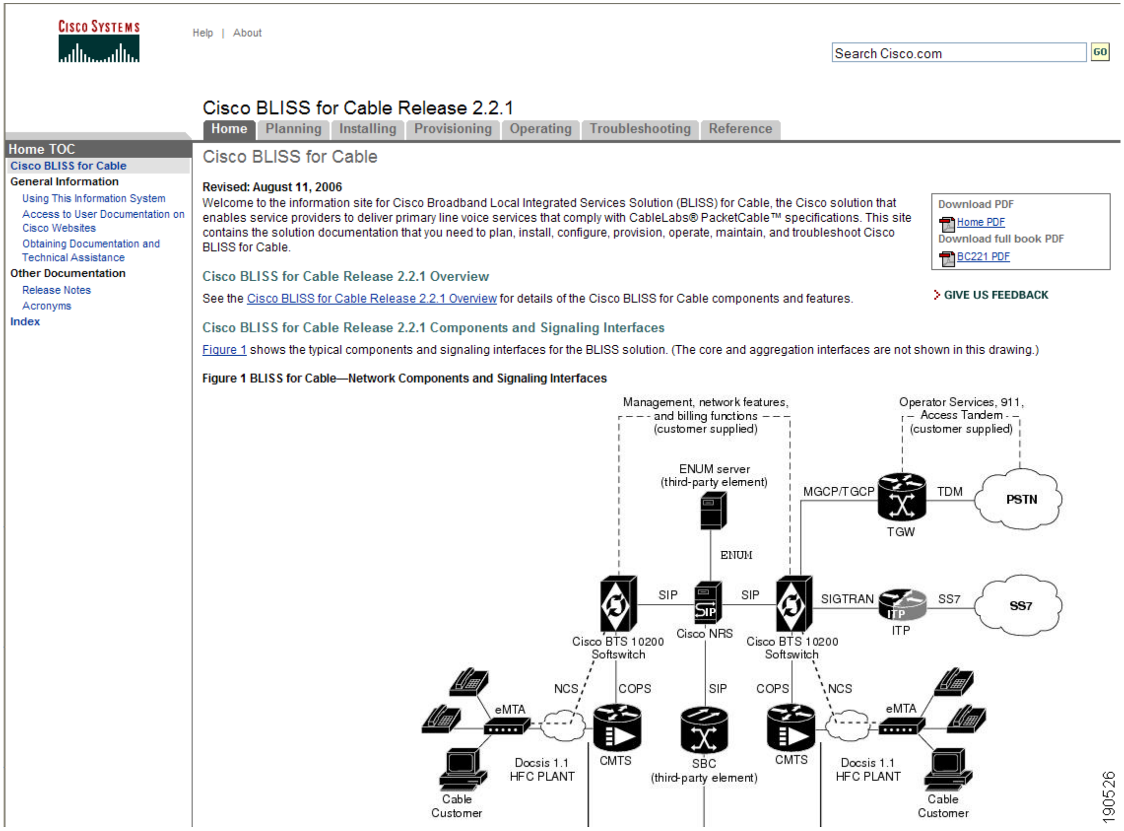
- Solution-Level Documentation
- Access to Password-Protected Documentation on Cisco Websites

Solution-Level Documentation

The solution-level documentation is available in the *Cisco BLISS for Cable Release 2.2.1 Information Access Manager (IAM)*. This IAM is a Web-based interface for accessing all Cisco BLISS for Cable Release 2.2.1 documentation, including requirements, procedures, feature descriptions, and so forth.

Figure 1 shows an image of the home page. The tabs across the top of the page represent the major tasks (Planning, Installing, Provisioning, Operating, and Troubleshooting) along with Home and Reference. The table of contents (TOC) in the left margin provides links to subsections.

Figure 1 Cisco BLISS for Cable Release 2.2.1 IAM Home Page (Partial View)



Cisco BLISS for Cable Release 2.2.1

Home TOC

Cisco BLISS for Cable

General Information

- Using This Information System
- Access to User Documentation on Cisco Websites
- Obtaining Documentation and Technical Assistance

Other Documentation

- Release Notes
- Acronyms

Index

Cisco BLISS for Cable

Revised: August 11, 2006

Welcome to the information site for Cisco Broadband Local Integrated Services Solution (BLISS) for Cable, the Cisco solution that enables service providers to deliver primary line voice services that comply with CableLabs® PacketCable™ specifications. This site contains the solution documentation that you need to plan, install, configure, provision, operate, maintain, and troubleshoot Cisco BLISS for Cable.

Cisco BLISS for Cable Release 2.2.1 Overview

See the Cisco BLISS for Cable Release 2.2.1 Overview for details of the Cisco BLISS for Cable components and features.

Cisco BLISS for Cable Release 2.2.1 Components and Signaling Interfaces

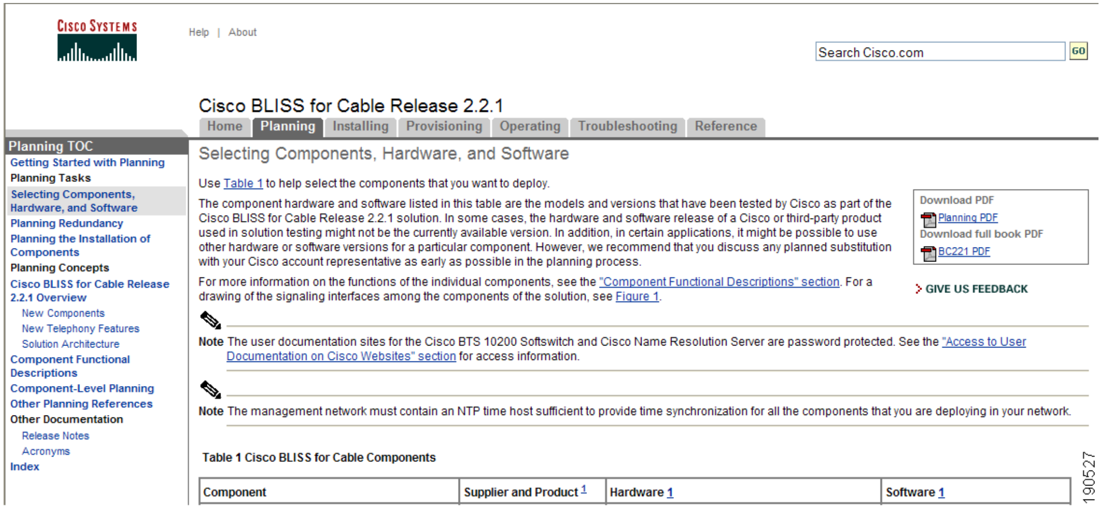
Figure 1 shows the typical components and signaling interfaces for the BLISS solution. (The core and aggregation interfaces are not shown in this drawing.)

Figure 1 BLISS for Cable—Network Components and Signaling Interfaces

Management, network features, and billing functions (customer supplied)
Operator Services, 911, Access Tandem (customer supplied)
ENUM server (third-party element)
MGCP/TGCP
TDM
PSTN
TGW
ENUM
SIP
SIP
SIGTRAN
SS7
SS7
ITP
ITP
Cisco BTS 10200 Softswitch
Cisco NRS
Cisco BTS 10200 Softswitch
NCS
COPS
SIP
COPS
NCS
eMTA
eMTA
CMTS
SBC (third-party element)
CMTS
Docsis 1.1 HFC PLANT
Docsis 1.1 HFC PLANT
Cable Customer
Cable Customer
190526

Figure 2 shows an IAM page with the Planning tab selected. Notice that the Cisco BLISS for Cable Release 2.2.1 Overview subsection (in the left margin) has also been selected. The IAM allows you to navigate directly to the desired information.

Figure 2 Cisco BLISS for Cable Release 2.2.1 IAM Planning Page with Subsection Selected in the Planning TOC



Selecting Components, Hardware, and Software

Use Table 1 to help select the components that you want to deploy.

The component hardware and software listed in this table are the models and versions that have been tested by Cisco as part of the Cisco BLISS for Cable Release 2.2.1 solution. In some cases, the hardware and software release of a Cisco or third-party product used in solution testing might not be the currently available version. In addition, in certain applications, it might be possible to use other hardware or software versions for a particular component. However, we recommend that you discuss any planned substitution with your Cisco account representative as early as possible in the planning process.

For more information on the functions of the individual components, see the "Component Functional Descriptions" section. For a drawing of the signaling interfaces among the components of the solution, see Figure 1.

Note The user documentation sites for the Cisco BTS 10200 Softswitch and Cisco Name Resolution Server are password protected. See the "Access to User Documentation on Cisco Websites" section for access information.

Note The management network must contain an NTP time host sufficient to provide time synchronization for all the components that you are deploying in your network.

Table 1 Cisco BLISS for Cable Components

Component	Supplier and Product [1]	Hardware 1	Software 1

Access to Password-Protected Documentation on Cisco Websites

The user documentation sites for the Cisco BTS 10200 Softswitch and the Cisco Name Resolution Server (NRS) are password protected.

- For access to the Cisco BTS 10200 Softswitch documentation, see your Cisco representative.
- For access to the Cisco NRS documentation on Cisco.com, take either of the following actions:
  - Apply for a Cisco.com login. Qualified users can establish an account on Cisco.com by following the directions found at this location: http://tools.cisco.com/RPF/register/register.do.
  - Send your User ID and Password (Login Name) in an email to: cscp-docs@external.cisco.com to obtain permission. If you have feedback about the documentation, please use this email address to send us the feedback.

Note If you have already logged into the Cisco site with a guest username and password for the Cisco BTS 10200 Softswitch, you may receive an error message when attempting to access other Cisco sites (sites requiring individual passwords). If you receive an error message, close all open instances of your browser, restart your browser program, and log into the desired Cisco site with the appropriate username and password.

Prerequisites for Using the Cisco BLISS for Cable Solution

Verify that all components you plan to deploy are compatible with the Cisco BLISS for Cable solution.

Verify that all of the components have been upgraded (if necessary) to the appropriate release as listed in the documentation.

Verify that the Cisco BTS 10200 Softswitch, the Cisco Name Resolution Server, and other components have been deployed with the proper level of redundancy and network path diversity.

Caution If components are not selected and installed according to the documented requirements, a traffic interruption could occur.

These prerequisites are discussed in detail in the Planning and Installation parts of the *IAM*.

Exceptions and Limitations—Selected Cases

This section highlights certain exceptions and limitations regarding features, deployment, and operation of this solution. It is not intended to be an exhaustive list. For access to all open and resolved caveats for the Cisco BLISS for Cable solution, see the "Caveats and Bug Toolkit" section on page 6.

Need to Reload the Configuration File Every Time After Restarting NRS

If you stop and start the NRS, routing policies are not loaded. The NRS issues the following error message: 404 routing policy has no algorithm. You must clear the persistent and reload the configuration file after each restart.

See caveat number CSCse49813. It is specific to Release 4.0.3.16 of the NRS.

Note The complete documentation for the Cisco NRS is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/cscp/30/dsnrs30.pdf. This documentation is password protected. To obtain access, see the "Access to Password-Protected Documentation on Cisco Websites" section on page 3.

Module-Trigger Configurations Lost after NRS Restart

After you upgrade to NRS version 4.0.3.x (up to version 4.0.3.16), and restart the NRS, the module-trigger configurations are lost. Without the module-trigger commands, the stand-alone NRS cannot route calls properly. In this situation, after restarting the NRS, you must reconfigure the module-trigger configurations.

See caveat number CSCse53306. It is specific to Release 4.0.3.16 of the NRS.

Features Delivered on SIP Ingress Requiring Calling Party Identity

For all calls incoming to the Cisco BTS 10200 Softswitch over a SIP trunk group (TG), features that require the calling party identification (such as automatic recall, automatic callback, customer originated trace, and so forth), are supported only if one of the following is true:

- The USE-PAI-HDR-FOR-ANI token is set to N in the applicable incoming softswitch TG table of the Cisco BTS 10200 Softswitch.

  or

- The USE-PAI-HDR-FOR-ANI token is set to Y in the applicable incoming softswitch TG table of the Cisco BTS 10200 Softswitch and the incoming SIP INVITE contains the P-Asserted ID (PAID) header.

See caveat number CSCsd07780.

CNAB for Outbound Calls on SIP Trunks

The Calling Name Blocking (CNAB) feature does not work for calls going out to SIP trunks. This is due to a SIP protocol limitation.

See caveat number CSCsa81305.

ENUM Server Availability Required if NRS Uses ENUM Routing Policy

By design, if ENUM routing policy is used on the NRS and all ENUM servers became unavailable, the NRS does not policy advance and those calls will fail. Therefore, if you have other routing policies configured on the NRS in addition to ENUM, and you want the system to invoke those policies in case the ENUM server lookup returns a name not found, you must ensure that at least one of the ENUM servers is always available.

See caveat number CSCsc63063.

Use of 302 Redirection and 503 Reject Messages in the NRS

The NRS allows the configuration of 302 redirection upon either a shutting-down or overload condition. However, the contact: header in the 302 redirect response does not contain any user-part information, therefore the Cisco BTS 10200 Softswitch is not able to redirect the call to another NRS. Because of this limitation, we recommend that you not configure the NRS to send a 302 message for shutting-down or overload condition when the NRS is interworking with the Cisco BTS 10200 Softswitch. Instead, we recommend that you use the 503 reject message. In this case the NRS rejects the call with the 503 response, and the Cisco BTS 10200 Softswitch uses an existing mechanism to retry another NRS node when it receives the 503 response.

See caveat number CSCsd90244.

Occasional Slow Response on NRS when Operating at Greater Than 65cps/tps with Large SIP Messages

A slow-response or congestion condition can occur on the NRS under the following conditions:

- The NRS is processing incoming requests continuously at the rate of more than 65 calls per second (or 65 transactions per second if NRS does not record-route).
- The SIP messages are large (more than 1000 bytes).
- The system is set at the default jvm maximum heap memory of 512 MB.

Under the conditions listed above, occasionally the NRS will take more than 500 ms to respond to incoming INVITE requests with “100 Trying.” This can cause the originating SIP client to time out and retransmit the INVITE request. The condition can cause intervals of several seconds (up to 5 seconds) between consecutive INVITE requests; following that, the NRS might normalize and resume normal operation, that is, the NRS responds to the incoming INVITE with “100 Trying” within the 500 ms retransmission window.

As a workaround, for NRS deployments in networks with high call rates and large SIP messages size, we recommend that, after consulting with your Cisco technical representative, you consider setting the maximum jvm heap memory for the NRS to at least 1280 MB. The maximum jvm heap memory for the NRS is set from the <install-path>/bin/dsnrs_env.sh script.

⚠ **Caution** Consult with your Cisco technical representative before making any changes to <install-path>/bin/dsnrs_env.sh script.

For redundancy, always deploy the NRS in a cluster of more than two, and configure the SIP client peer to load-balance the INVITE requests between members in the NRS cluster. In addition, if possible, configure the SIP client peer to retransmit a timed-out INVITE to different member in the NRS cluster. This helps to avoid long post-dial delay.

For the configuration procedure, see "Adjusting the Memory Allocation" in the Installation chapter of the *Name Resolution Server Administrator's Guide*.

See caveat number CSCse28891.

CALEA Functionality

The following are the known limitations to providing CALEA compliance in Cisco BLISS for Cable Release 2.2.1. These are deemed to fall under the 18-month "safe harbor" exemption issued by the FCC in August, 2005. This functionality will be provided in Release 5.0 of the Cisco BTS 10200 Softswitch.

- No call content is tapped on calls forwarded outside of the CMS to which the targeted subscriber is locally attached. This is true if the call is forwarded to the PSTN or to another NCS endpoint on another CMS, for example:

  User-C/User-P/User-X -> MGC/CMS2 -> NRS -> CMS1 -> UserA(forwarded) -> NRS -> MGC/CMS2 -> User-Q/User-Y

- No call content is tapped on NCS or PSTN calls forwarded to voicemail when the PSTN ingress MGC or calling party CMS, and the called party's CMS and VM SIP trunk, are not all the same Cisco BTS 10200 Softswitch. For example:

  User-C/User-P/User-X -> MGC/CMS2 -> NRS -> CMS1 -> User A(CFNA to VM) -> VM

  In this situation, CALEA compliance is provided only when the CMS and MGC are not separated. Perform the tap at the MGW in the PSTN case, and on the calling party CMTS in the NCS case. For example:

  User-C/User-P -> MGC/CMS1 -> NRS (only for User-P's call) -> CMS1 -> User A(CFNA to VM) -> VM

- The treatment of call data depends on the status of targeted subscriber:
  - For calls placed to/from a targeted NCS subscriber locally attached to that CMS, call data is sent by the CMS to the CALEA DF (Distribution Function).
  - For calls terminated via, or ingressed from, an MGC on a different Cisco BTS 10200 Softswitch than the CMS to which the targeted subscriber is locally attached, call data is *not* sent, because the MGC was not instructed (via LAES headers sent from the targeted subscriber CMS) to send such call data to the DF.

For additional details about specific CALEA functions, limitations, and configuration in the BLISS for Cable 2.2.1 solution, contact your Cisco account team.

Caveats and Bug Toolkit

Open and resolved caveats are not listed in this Release Notes document. Instead, the latest information on caveats is available through an online tool, Bug Toolkit, available for customers to query caveats according to their own needs.

To access Bug Toolkit, you must have an Internet connection and a web browser, as well as a Cisco.com username and password. See your Cisco representative if you need assistance obtaining a username and password.

To use Bug Toolkit, follow this procedure.

Step 1 Click here to log in to Bug Toolkit. You must have a Cisco.com username and password.

> **Note** If you have already logged into www.cisco.com with the BTS guest username and password, you might receive an error message when attempting to access the Bug Toolkit. If you receive an error message, close all open instances of your browser, restart your browser program, and log into www.cisco.com with your own registered username and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for the Cisco BTS 10200 Softswitch, for example, go to the "Search for bugs in other Cisco software and hardware products" section, and start typing **BTS** in the Product Name field. The Cisco BTS 10200 Softswitch listing should appear after typing the first two letters, **B** and **T**.

Step 4 Click **Next**. The Cisco BTS 10200 Softswitch search page appears.

Step 5 Select the filters to query for caveats. You can choose any or all of the available options:

> **Note** To make less specific queries, you can simply leave the default "All" option for the Major/Minor release, Features/Components, and keyword options; however, you should be aware that general queries may take longer and may return a large number of caveats. Be as specific as necessary in setting options.

Step 6 By version:

- Select **Major** for the major releases, such as 4.5.
- Select **Minor Release** for more specific information—for example, selecting Major version 4.5 and Minor version 1 queries specifically for Release 4.5.1 caveats.
- Select the **Features or Components** to query.
- Use keywords to search for a caveat title and description.
- Select the **Advanced Options**, including the Bug Severity level, Bug Status Group, and Release Note Enclosure options.
- Click **Next**.

  Bug Toolkit returns a list of caveats based on your query.

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/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 comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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 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 at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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 (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 & Documentation 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 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 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 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

- *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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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 for networking professionals to 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

- 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.