Release Notes for Catalyst 6500 Series Switch WebVPN Services Module Software Release 1.x

Current Release: 1.2(1)—November 16, 2005
Previous releases: 1.1(1a), 1.1(1)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series WebVPN Services Module software release 1.*x*.

Note For detailed installation and configuration procedures for the WebVPN Services Module, refer to the Catalyst 6500 Series WebVPN Services Module documentation at this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/webvpn/index.htm

Contents

This document consists of these sections:

- System Requirements, page 2
- Orderable Software Images, page 2
- Client Packages, page 3
- New Features in Software Release 1.2, page 3
- Features in Software Release 1.1, page 4
- Limitations and Restrictions, page 8
- Open and Resolved Caveats in Software Release 1.2(1), page 9
- Open and Resolved Caveats in Software Release 1.1(1a), page 10
- Open and Resolved Caveats in Software Release 1.1(1), page 11
- Related Documentation, page 12
- Obtaining Documentation, page 13

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

- Documentation Feedback, page 14
- Cisco Product Security Overview, page 14
- Obtaining Technical Assistance, page 15
- Obtaining Additional Publications and Information, page 16

System Requirements

This section describes the system requirements for the Catalyst 6500 series WebVPN Services Module software release 1.x:

- Hardware Requirements, page 2
- Software Requirements, page 2

Hardware Requirements

The WebVPN Services Module is supported in systems with a Supervisor Engine 32 or Supervisor Engine 720, and with any module with ports that connect server and client networks.

Software Requirements

Table 1 lists the WebVPN Services Module software versions supported by Cisco IOS software.

Table 1 WebVPN Services Module Software Compatibility

Product Number	Minimum WebVPN Software Version		Recommended WebVPN Software Version		Minimum Cisco IOS Software
WS-SVC-WEBVPN-K9	Application Image	Maintenance Image	Application Image	Maintenance Image	
• Supervisor Engine 720	1.1(1)	3.3(1)	1.2(1)	3.3(1)	12.2(18)SXE2 12.2(17d)SXB7
• Supervisor Engine 32	1.1(1)	3.3(1)	1.2(1)	3.3(1)	12.2(18)SXF

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the WebVPN Services Module software.

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number
1.2(1)	c6svc-webvpn-k9y9.1-2-1.bin	SC-SVC-WVPN-12-K9
1.1(1a)	c6svc-webvpn-k9y9.1-1-1a.bin	SC-SVC-WVPN-11-K9
1.1(1)	c6svc-webvpn-k9y9.1-1-1.bin	SC-SVC-WVPN-11-K9

Client Packages

This section describes where to download the client packages and where to find more information about installing the client packages on the gateway.

SSL VPN Client Package

You can download the SSL VPN client (SVC) package (sslclient-win-1.0.0.179.pkg) from this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des

For information about installing the SVC package with WebVPN software release 1.2(*x*), refer to the "SVC Package for Tunnel Mode" section at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/webvpn/1_2/config/upgrade.htm

For information about installing the SVC package with WebVPN software release 1.1(*x*), refer to the "Installing the SVC Package for Tunnel Mode" section at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/webvpn/1_1/config/upgrade.htm

Cisco Secure Desktop Package

You can download the Cisco Secure Desktop package (securedesktop_cat6k_3_1*.pkg) from this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

For information about installing the CSD package with WebVPN software release 1.2(*x*), refer to the "Cisco Secure Desktop Package" section at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/webvpn/1_2/config/upgrade.htm

New Features in Software Release 1.2

This section describes the new features available in WebVPN software release 1.2:

- Support for Cisco Secure Desktop (CSD)—CSD provides a consistent and reliable means of eliminating all traces of sensitive data by providing a single, secure location for session activity and removal on the client system.
- Citrix server integration
- Support for up to 8000 end users with license upgrade
- Support for up to 128 virtual contexts
- Run-time software upgrades—Allows you to upgrade the client images (CSD and SSL VPN client) while allowing client downloads at the same time.
- Log level filter—Allows you to filter the level of system messages that are logged, based on severity level (normal, critical, or fatal).
- Support for authentication proxy for basic and NT LAN Manager (NTLM) authentication
- Support for Japanese Shift-JIS encoding for Common Internet File System (CIFS)

Features in Software Release 1.1

Table 3 describes the initial feature set in WebVPN Services Module software release 1.1.

Table 3 Feature Set Description

Features
Supported Supervisor Engine Hardware
Supervisor Engine 720
Supported Software
Cisco IOS Release 12.2(17d)SXB7 or later releases on Supervisor Engine 720
WebVPN Services Module software release 1.1(1) or later releases on the WebVPN Services Module
Supported Web Browsers
Microsoft Internet Explorer 6.0
Netscape Navigator 7.2
Supported End User Operating Systems
Windows XP
Windows 2000 Professional
Linux Red Hat 9.0
Secure Transport Protocol
SSL 3.0
SSL 3.1/TLS[1] 1.0
Cipher Suite
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CSC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA

Table 3 Feature Set Description (continued)

Features
Client Models
Clientless Mode: – URL Mangling – Cookie Mangling – WebDAV[2] Mangling – XML Mangling – Javascript Mangling
Thin-client Mode (also called TCP port-forwarding [Java])
Tunnel Mode: – No PC reboot required – Web-based client download (less than 500 kB) – SVC[3] binary is Microsoft-signed – Supports Windows 2000 and Windows XP – Supports the option to keep SVC[3] installed on a client PC – Split tunnel – SSL rekey
Applications Support
Clientless Mode: – Web-access (HTTP/HTTPS) – File service (CIFS[4]) – Microsoft OWA[5] (OWA 5.5, OWA 2000, OWA 2003)
Thin-client Mode: – Applications that use static TCP ports (Telnet, SSH[6], SMTP[7], POP3[8], IMAP4[9], Sametime, Meeting Maker, and so on)
Tunnel Mode – All IP-based applications (except those that require IP mulitcast)
Virtualization
Supports 64 virtual contexts
Supports 64 virtual gateways
User-to-context mapping – IP address based – URL and virtual hostname based – Login name based – URL pathname based

Table 3 Feature Set Description (continued)

Features
VRF[10] Awareness
Per-VRF AAA[11] server
Per-VRF DNS[12] server
Per-VRF default gateway
Per-VRF maximum users enforcement
User Authentication
Radius
User-to-group mapping through an external database
Network Access Control
IP address
DSCP[13]/ToS[14]
Protocol
TCP/UDP port
Per user
Per group
Bookmarking
Administrator bookmarking (group level)
End-system Integrity
Disable browser caching
Disable auto complete
Cookie invalidation
Capacity and Performance
Up to 8000 concurrent users (licensing required)
Up to 290-Mbps throughput
Up to 32000 concurrent connections
Scalability (4 modules per chassis)
Redundancy and Load Sharing
Cisco IOS SLB[15] integration
CSM[16] integration
Configuration and Management
Console CLI
Telnet
SSH
syslog Support
Console display
External server
Internal buffer (wrap support)

Table 3 Feature Set Description (continued)

Features
Public Key Infrastructure
RSA key pair generation for certificates up to 2048 bits
Secure key storage in WebVPN Services Module Flash memory device
Certificate enrollment for client and server-type proxy services
Importing and exporting of key and certificate (PKCS12 and PEM)
Duplicating keys and certificates on WebVPN Services Module using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring keys and certificates
Auto-enrollment and auto-renewal of certificates
Importing of certificate authority certificates by cut-and-paste or TFTP
Up to 8 levels of certificate authority in a certificate chain
Manual certificate enrollment using cut-and-paste or TFTP of PKCS10 CSR file
Server certificate authentication
Server certificates
Certificate security attribute-based access control lists
CRL[17]
High Availability
Failure detection (SLB health monitoring schemes)
System-level redundancy (stateless) (when used with the CSM)
Module-level redundancy (stateless) (when used with the CSM or with multiple WebVPN Services Modules configured with HSRP [18])
Serviceability
OIR[19] (after a proper shutdown)
Graceful shutdown
Password recovery

1. TLS = Transport Layer Security
2. WebDAV = WWW Distributed Authoring and Versioning
3. SVC = SSL VPN client
4. CIFS = Common Internet File System
5. OWA = Outlook Web Access
6. SSH = Secure Shell
7. SMTP = Simple Mail Transfer Protocol
8. POP3 = Post Office Protocol version 3
9. IMAP4 = Internet Message Access Protocol version 4
10. VRF = VPN routing and forwarding
11. AAA = Authentication, Authorization, and Accounting
12. DNS = Domain Name System
13. DSCP = Differentiated Services Code Point

14. ToS = Type of Service
15. SLB = Server Load Balancing
16. CSM = Content Switching Module
17. CRL = Certificate Revocation List
18. HSRP = Hot Standby Routing Protocol
19. OIR = Online Insertion and Removal

Limitations and Restrictions

This section describes general limitations and restrictions:

- The output of the **show interfaces webvpn 0** command does not correctly display traffic statistics. To accurately monitor the traffic across the WebVPN Services Module, enter the **show webvpn module** *mod* **traffic** command from the supervisor engine console.
- If the time zone setting on a Windows file server is different from the time zone setting on the WebVPN gateway, the time displayed for “File last modified” or “Folder last modified” will be different between the file server and the gateway.
- The WebVPN gateway does not impose a limitation on filename length during file upload. However, Microsoft Internet Explorer 6.0 limits the filename to 253 characters; Netscape Navigator 7.2 limits the filename to 256 characters.
- The Outlook Web Access (OWA) calendar in Exchange 5.5 does not display properly when you configure TLS1 for the SSL version of the gateway. The Java plug-in only uses SSL3. Configure the gateway to use SSL3.
- If an end user accesses a long email that contains about 10,000 lines of text (about 400 kb in file size) from the Exchange 2000 server, the browser might fail to respond. The problem does not occur with emails that contain large attachments.

  Workaround: Close the browser window and start a new browser session.
- You cannot import a partial certificate chain, you need to import the entire certificate chain.
- Cisco Discovery Protocol (CDP) is not supported on the WebVPN Services Module; however, the CLI is available.
- Do not enable debugging when the WebVPN Services Module is experiencing high traffic loads.
- Tunnel mode allows 200 split-include and split-exclude configurations on the module. However, the same number of configurations cannot be retrieved from the RADIUS server during authentication because the RADIUS protocol defines a size limit of 4096 bytes. If the total length of all the group policy attributes exceeds 4096 bytes, the RADIUS server ignores the rest of the attributes.

  Workaround: Configure the split-include and split-exclude configurations in the group policy, and then retrieve the group policy name from the RADIUS server.
- The Outlook Web Access (OWA) inbox might not load properly.

  Workaround: Upgrade to Exchange Server 2003 Service Pack 2.

Open and Resolved Caveats in Software Release 1.2(1)

These sections describe open and resolved caveats in WebVPN Services Module software release 1.2(1):

- Open Caveats in Release 1.1(1a), page 10
- Resolved Caveats in Release 1.1(1a), page 11

Open Caveats in Release 1.2(1)

This section describes open caveats for the WebVPN Services Module software release 1.2(1).

- A stateful switchover (SSO) will reset the WebVPN Services Module. (CSCeh62196)
- When end users use the WebVPN portal page to browse a domain that contains more than 2500 servers, only 2500 servers are displayed.

  Workaround: In the file-entry box on the portal page, end users can enter the following:

  – *server* — Displays all shares under this server

  – *server**share*—Displays all files and folders under this share (CSCeg57753)
- When you reset the WebVPN Services Module from a supervisor engine that is running Cisco IOS software release 12.2(17d)SXB7 or later, the following message displays on the supervisor engine console:

  `Received unknown unsolicited message from module mod, opcode 0x330`

  This problem does not affect the functionality of the WebVPN Services Module. (CSCin90232)
- When you browse a domain, a UDP request and reply exchange occurs with the master browser. When the interface or VLAN on which this exchange occurs is brought down before the exchange completes, or when the ARP entry for the NAT address is removed, the supervisor engine drops the UDP reply. The gateway does not attempt to retry this exchange. This problem can cause browser errors to occur and the browse domain to fail.

  Workaround: Click the **OK** button on the error page, and retry the operation. (CSCeh69890)
- If you enable SSHv2 and export a certificate using SCP, the export process can take up to 6 minutes.

  Workaround 1: Use a different file system to export the certificate.

  Workaround 2: Enable SSHv1. (CSCsb09985)
- If you enable SSHv2 and import a certificate using SCP, the import process might fail.

  Workaround 1: Use a different file system to import the certificate.

  Workaround 2: Enable SSHv1. (CSCsb10016)
- If you upload a file to a remote fileserver through the WebVPN gateway by entering a filename that does not exist locally, a file is created with zero bytes on the remote file server. (CSCeg59735)
- Because of web browser limitations, the WebVPN session might expire if too many server-generated cookies pass through the WebVPN gateway.

  Workaround: Log in again to the gateway. (CSCej10098)
- You will not be able to log in to the CSD (Cisco Secure Desktop) manager if a previous CSD manager session is not properly logged out. The CSD manager does not allow multiple administrator sessions.

  Workaround: Enter the **clear webvpn session user admin context Default_context** command on the gateway. (CSCsb80160)

Resolved Caveats in Release 1.2(1)

This section describes resolved caveats in WebVPN Services Module software release 1.2(1):

- You cannot configure a banner for a specific group; however the **banner** CLI is available.

  Workaround: Enter the **title** command for the entire context.

  This problem is resolved in WebVPN Services Module software release 1.2(1). (CSCei11191)

Open and Resolved Caveats in Software Release 1.1(1a)

These sections describe open and resolved caveats in WebVPN Services Module software release 1.1(1a):

- Open Caveats in Release 1.1(1a), page 10
- Resolved Caveats in Release 1.1(1a), page 11

Open Caveats in Release 1.1(1a)

This section describes open caveats for the WebVPN Services Module software release 1.1(1a).

- An SSO redundancy switchover will reset the WebVPN Services Module. (CSCeh62196)
- You cannot configure a banner for a specific group; however the **banner** CLI is available.

  Workaround: Enter the **title** command for the entire context. (CSCei11191)
- When end users use the WebVPN portal page to browse a domain that contains more than 2500 servers, only 2500 servers display.

  Workaround: In the file-entry box on the portal page, end users can enter the following:

  – *server* — Displays all shares under this server

  – *server**share*—Displays all files and folders under this share (CSCeg57753)
- When you reset the WebVPN Services Module from a supervisor engine that is running Cisco IOS software release 12.2(17d)SXB7 or later rebuilds, you will see the following message displayed on the supervisor engine console:

  `Received unknown unsolicited message from module` *`mod`*`, opcode 0x330`

  This problem does not affect the functionality of the WebVPN Services Module. (CSCin90232)
- When you browse a domain, a UDP request and reply exchange occurs with the master browser. When the interface or VLAN on which this exchange is brought down before the exchange completes, or when the ARP entry for the NAT address is removed, the UDP reply is dropped by the supervisor engine. The gateway does not attempt to retry this exchange. This problem can cause Browse Errs to occur and the browse domain to fail.

  Workaround: Click the **OK** button on the error page and retry the operation. (CSCeh69890)
- If you enable SSHv2 and export a certificate using SCP, the export process can take up to 6 minutes.

  Workaround 1: Use a different file system to export the certificate.

  Workaround 2: Enable SSHv1. (CSCsb09985)

- If you enable SSHv2 and import a certificate using SCP, the import process might fail.

  Workaround 1: Use a different file system to import the certificate.

  Workaround 2: Enable SSHv1. (CSCsb10016)
- If you upload a file to a remote fileserver through the WebVPN gateway by entering a filename that does not exist locally, a file is created with zero bytes on the remote file server. (CSCeg59735)

Resolved Caveats in Release 1.1(1a)

This section describes resolved caveats in WebVPN Services Module software release 1.1(1a):

- When you enter the **no nbns-list** command to delete an NBNS list, the following error message is displayed:

  ```
  Error nbns-list is referenced in 1 group policies, remove the reference first.
  ```

  This problem is resolved in WebVPN Services Module software release 1.1(1a). (CSCin95384)

Open and Resolved Caveats in Software Release 1.1(1)

These sections describe open and resolved caveats in WebVPN Services Module software release 1.1(1):

- Open Caveats in Release 1.1(1), page 11
- Resolved Caveats in Release 1.1(1), page 12

Open Caveats in Release 1.1(1)

This section describes open caveats for the WebVPN Services Module software release 1.1(1).

- An SSO redundancy switchover will reset the WebVPN Services Module. (CSCeh62196)
- You cannot configure a banner for a specific group; however, the **banner** CLI is available.

  Workaround: Enter the **title** command for the entire context. (CSCei11191)
- When end users use the WebVPN portal page to browse a domain that contains more than 2500 servers, only 2500 servers display.

  Workaround: In the file-entry box on the portal page, end users can enter the following:

  – *server*—Displays all shares under this server

  – *server**share*—Displays all files and folders under this share (CSCeg57753)
- When you reset the WebVPN Services Module from a supervisor engine that is running Cisco IOS software release 12.2(17d)SXB7 or later, the following message displays on the supervisor engine console:

  ```
  Received unknown unsolicited message from module mod, opcode 0x330
  ```

  This problem does not affect the functionality of the WebVPN Services Module. (CSCin90232)

- When you browse a domain, a UDP request and reply exchange occurs with the master browser. When the interface or VLAN on which this exchange occurs is brought down before the exchange completes, or when the ARP entry for the NAT address is removed, the supervisor engine drop the UDP reply. The gateway does not attempt to retry this exchange. This problem can cause Browse Errs to occur and the browse domain to fail.

  Workaround: Click the **OK** button on the error page and retry the operation. (CSCeh69890)

- If you enable SSHv2 and export a certificate using SCP, the export process can take up to 6 minutes.

  Workaround 1: Use a different file system to export the certificate.

  Workaround 2: Enable SSHv1. (CSCsb09985)

- If you enable SSHv2 and import a certificate using SCP, the import process might fail.

  Workaround 1: Use a different file system to import the certificate.

  Workaround 2: Enable SSHv1. (CSCsb10016)

- If you upload a file to a remote fileserver through the WebVPN gateway by entering a filename that does not exist locally, a file is created with zero bytes on the remote file server. (CSCeg59735)

Resolved Caveats in Release 1.1(1)

There are no resolved caveats in WebVPN Services Module software release 1.1(1).

Related Documentation

For additional information about Catalyst 6500 series switches and command-line interface (CLI) commands, refer to the following publications:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Switch WebVPN Services Module Installation and Verification Note*
- *Catalyst 6500 Series Switch WebVPN Services Module Configuration Guide*
- *Catalyst 6500 Series Switch WebVPN Services Module Command Reference*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2*
- For information about MIBs, refer to this URL:

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

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

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

  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.

- 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 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 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.

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)—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, 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

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