Release Notes for Cisco VPN 3002 Hardware Client Release 3.5

These release notes describe the features of the Cisco VPN 3002 Hardware Client and the caveats that apply for Release 3.5. Read the release notes carefully prior to installation.

Contents

These release notes include the following topics:

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

Introduction

The Cisco VPN 3002 Hardware Client (referred to in these Release Notes as the VPN 3002) communicates with a VPN 3000 Series Concentrator to create a virtual private network across a TCP/IP network (such as the Internet). The VPN 3002:

- Provides an alternative to deploying the VPN Client at remote locations.
- Is located at a remote site (like the VPN Client).
- Provides a secure connection to a VPN 3000 Concentrator at a central site.
- Requires minimal configuration.

The secure connection between the VPN 3002 and the VPN Concentrator is called a *tunnel*. The VPN 3002 uses the IPSec protocol to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. It can support a single IP network.

The VPN 3002 Hardware Client provides an alternative to deploying the VPN Client software to PCs at remote locations. Like the software client, the VPN 3002 is located at a remote site, and provides a secure connection to a Concentrator at a central site. It is important to understand that the VPN 3002 is a hardware *client*, and that you configure it as a client, not as a site-to-site connection.

System Description

The following sections describe the VPN 3002 hardware.

Physical Site Requirements

The VPN 3002 requires a normal computing-equipment environment, including power requirements. For maximum protection, we recommend connecting it to a conditioned power source or UPS (uninterruptible power supply). Be sure that the power source provides a reliable Earth ground.

Physical Specifications

- Width: 8.85 inches (22.48 cm)
- Depth: 7 inches (17.78 cm)
- Height: 2.12 inches (5.38 cm)
- Weight: 2.25 lb. (1.02 kg)
- External power supply:
  - Input: 100 to 240 VAC at 50/60 Hz (autosensing)
  - Output: 3.3 v @ 4 amps
- Cooling: Normal operating environment, 32^{o} to 122^{o}F (0^{o} to 50^{o}C), convection only; cooling intake vents are on the sides and top. Allow at least 3 inches (75 mm) of unobstructed space on all sides.
- Cabling distances from an active network device: approximately 328 feet (100 meters)
- UL approved: electrical, mechanical, and construction
- FCC, E.U., and VCCI Class B compliance

Installation Notes

For complete installation information, refer to the *VPN 3002 Hardware Client Getting Started* guide. To install and configure the VPN 3002 using default values, see the *VPN 3002 Quick Start* card, which ships with the VPN 3002.

Initial Configuration

You must meet these requirements to configure the VPN 3002.

Central-site VPN Concentrator Requirements

To interoperate with a VPN 3002, the VPN 3000 Series Concentrator to which it connects must:

- Be running software version 3.0 or later. For most features new in software version 3.5, you must be running version 3.5 software on both the VPN 3002 and on the VPN Concentrator to which it connects.
- Configure IPSec group and user names and passwords for this VPN 3002.
- For a VPN 3002 running in PAT mode, enable a method of address assignment: DHCP, address pools, per user, or authentication server address.
- For a VPN 3002 running in Network Extension mode, use Reverse Route Injection, a VPN Concentrator feature new in Release 3.5, or configure on your central-site router a static route to the private network of the VPN 3002.

See Chapter 3, “Quick Configuration using the VPN 3002 Hardware Client Manager,” in the *VPN 3002 Hardware Client Getting Started* manual for step-by-step Quick Configuration instructions.

Configuration Interfaces

For easiest use, we strongly recommend using the VPN 3002 Hardware Client Manager (referred to in these Release Notes as the Manager), which is HTML-based, from a PC and browser. The PC must be able to run the recommended browser.

You can also configure and manage the VPN 3002 using:

- a PC attached to the console port via the command-line interface (CLI). The console can be the same PC that runs the browser.
- Telnet, Telnet/SSL, or SSH via the private LAN.
- An XML-based interface.

Browser Requirements

The VPN 3002 Hardware Client Manager works with the following browsers:

- Internet Explorer version 4.x and higher
- Netscape version 4.5 and higher

Be sure JavaScript and cookies are enabled in the browser. Whatever browser and version you use, install the latest patches and service packs for it.

Do not use the *browser* navigation toolbar buttons **Back, Forward**, or **Refresh / Reload** with the VPN 3002 Hardware Client Manager unless instructed to do so. To protect access security, clicking **Refresh / Reload** automatically logs out the Manager session. Clicking **Back** or **Forward** may display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN Concentrator Manager.

Recommended PC Monitor/Display settings

For ease of use, we recommend setting your monitor or display:

- Desktop area = 1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette = 256 colors or higher.

Hardware Features Summary

The VPN 3002 comes in two models, differentiated by number and type of Ethernet connections:

- **VPN 3002** — two 10/100 BaseT Ethernet ports (one public and one private port).
- **VPN 3002-8E** — one 10/100 BaseT Ethernet port on the public interface and a built-in 8-port 10/100 BaseT Ethernet switch at its private network connection.

All VPN 3002 systems have the following features:

- Motorola® PowerPC CPU
- SDRAM memory for normal operation
- Nonvolatile memory for critical system parameters
- Flash memory for file management
- Software-based encryption
- Single power supply
- Compact physical dimensions
- Desk-top or wall-mountable chassis

Release 3.5 New Software Features

The following sections describe software features new in Release 3.5.

IPSec over TCP

IPSec over TCP encapsulates encrypted data traffic within TCP packets. This feature enables the VPN 3002 to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls.

Note This feature does not work with proxy-based firewalls.

The VPN 3002 Hardware Client, which supports one tunnel at a time, can connect using either standard IPSec, IPSec over TCP, or IPSec over UDP.

To use IPSec over TCP, both the VPN 3002 and the VPN Concentrator to which it connects must be running version 3.5 software.

Interactive Hardware Client Authentication

Interactive hardware client authentication provides the central site with additional security by requiring the VPN 3002 to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled the VPN 3002 does not have a saved username and password.

When the VPN 3002 initiates the tunnel, it sends the username and password to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication on either the internal or an external server. If the username and password are valid, the tunnel is established.

You configure interactive hardware client authentication on a group basis on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the same LAN as the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists.

Note You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

- If your browser points to a default home page, or to a website on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.
- If you try to access resources on the network behind the VPN Concentrator that are not web-based, for example, email, the connection will fail until you authenticate.
- To authenticate if your browser does not automatically redirect you to the login pages, enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.

You configure individual user authentication on a group basis on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

RADIUS with Password Expiry

RADIUS with password expiry is an IPSec authentication method that you configure on a VPN Concentrator on a group basis. This option lets the VPN 3000 Concentrator that is attempting to authenticate an IPSec client to an external RADIUS server (acting as a proxy to an NT server) determine when a user's password has expired and prompt for a new password. By default, this option is disabled.

Enabling this option allows the VPN 3000 Concentrator to use MS-CHAP-v2 when authenticating an IPSec client to an external RADIUS server. That RADIUS server must support both MS-CHAP-v2 and the Microsoft Vendor Specific Attributes. Refer to the documentation for your RADIUS server to verify that it supports these capabilities.

Because of the use of MS-CHAP-v2, when this option is enabled on the VPN 3000 Concentrator, the VPN Concentrator can provide enhanced login failure messages that describe specific error conditions. These conditions are:

- Restricted login hours.
- Account disabled.
- No dialin permission.

- Error changing password.
- Authentication failure.

The “password expired” message appears when the user whose password has expired first attempts to log in. The other messages appear only after three unsuccessful login attempts.

Note To use RADIUS password expiry with a VPN 3002, you must enable interactive hardware client authentication. This feature does not work for individual user authentication.

Backup IPSec Servers

IPSec backup servers let a VPN 3002 Hardware Client connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002 or on a group basis at the VPN Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server list to the VPN 3002 hardware clients in the group.

Load Balancing

Load balancing lets you distribute sessions among two or more VPN Concentrators connected on the same network to handle remote sessions. Load balancing directs sessions to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability. Load balancing requires no configuration on the VPN 3002.

Simple Certificate Enrollment Protocol (SCEP)

You can enroll and install digital certificates on the VPN 3002 automatically or manually. The automatic method is a new feature that uses the Simple Certificate Enrollment Protocol (SCEP) to streamline enrollment and installation. SCEP is a secure messaging protocol that requires minimal user intervention. This method is quicker than enrolling and installing digital certificates manually, but it is available only if you are both enrolling with a CA that supports SCEP and enrolling via the web. If your CA does not support SCEP, or if you enroll with digital certificates by a means other than the web (such as through email or by a diskette), then you cannot use the automatic method; you must use the manual method.

Reset/Restore Monitoring Statistics

You can now reset and restore statistical data to better note changes in that data. When you click Reset on a monitoring or administration screen, the VPN 3002 temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle’s trip odometer, versus the regular odometer. Click Restore to return to the actual statistical values.

XML Management

VPN 3000 Concentrators and VPN 3002 Hardware Clients now support an XML-based interface to allow them to be more easily managed by an external management application.

This interface can be used by Cisco management applications, third-party applications that manage our products, and customers who want to manage their devices using their own infrastructure. This feature is enabled my default; you do not have to configure it.

The XML data can be sent to or uploaded from the VPN 3000 Concentrator using HTTPS, SSH, or standard file transfer mechanisms such as FTP or TFTP.

Reverse Route Injection (RRI)

You can configure the VPN 3000 Concentrator to add routes to its routing table for remote hardware or software clients. The VPN Concentrator can then advertise these routes to its private network via RIP or OSPF. This feature is called reverse route injection (RRI).

For example, with a VPN 3002 in network extension mode, network extension RRI automatically adds hosts on the VPN 3002 private network to the VPN Concentrator’s routing table for distribution by either RIP or OSPF.

RRI requires no configuration on the VPN 3002.

Software Features Summary

The VPN 3002 software includes the following software features.

- The VPN 3002 has two operating modes: Client/PAT mode and Network Extension mode. For more information, see the section on Client Mode and Network Extension Mode, below.
- IPSec is the tunneling protocol.
- IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature does not work with proxy-based firewalls.
- UDP NAT/FW Transparent IPSec enables secure transmission between the VPN 3002 Hardware Client and the central-site VPN Concentrator through a device, such as a firewall, that is performing Network Address Translation (NAT).
- Interactive hardware client authentication, when enabled, provides security by requiring that you manually enter a valid username and password for the VPN 3002 each time the VPN 3002 attempts to connect to a VPN Concentrator.
- Individual user authentication, when enabled, requires that individual users enter a valid username and password to access the network behind the central-site VPN Concentrator even though the tunnel already exists.
- IPSec backup servers let a VPN 3002 connect to a backup VPN Concentrator when its primary VPN Concentrator is unavailable.
- Load balancing lets you distribute traffic from remote clients among two or more VPN Concentrators.
- Reverse route injection (RRI) lets you configure the VPN Concentrator to add routes to its routing table for the VPN 3002 or software clients. The VPN Concentrator can then advertise these routes to its private network via RIP or OSPF.
- Radius with password expiry lets a VPN 3000 Concentrator that is attempting to authenticate an IPSec client to an external RADIUS server (acting as a proxy to an NT server) determine when a user’s password has expired and prompt for a new password.
- PPP over Ethernet (PPPoE) lets a network client interact with service provider equipment, such as a broadband modem, most often xDSL.

- The VPN 3002 has two management interfaces: HTML and command-line interface.
- The auto-update feature lets you upgrade software for multiple hardware clients from a single, central-site location.
- The VPN 3002 uses two encryption algorithms: 56-bit DES (Data Encryption Standard) and 168-bit Triple DES.
- The VPN 3002 uses two authentication algorithms:
  - MD5/HMAC-128: HMAC (Hashed Message Authentication Coding) with the MD5 (Message Digest 5) hash function using a 128-bit key.
  - SHA/HMAC-160: HMAC with the SHA-1 (Secure Hash Algorithm) hash function using a 160-bit key.
- Key management uses Internet Key Exchange (IKE) (formerly called ISAKMP/Oakley) with Diffie-Hellman key technique.
- Network addressing support uses DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) client and server.
- Support for multiple certificate authorities includes Baltimore, Entrust, Microsoft Windows 2000, Netscape, RSA Keon, and VeriSign.
- SCEP (Simple Certificate Enrollment Protocol) lets you enroll and install certificates automatically.
- XML Management lets external management applications administer the VPN 3002.
- Reset and Restore Monitoring lets you better note changes in statistical data.
- System administration features include session monitoring and management, software image update, system reset and reboot, PING capability, configurable system administrator profiles, and digital certificate management.
- Monitoring capabilities include event logging and notification via system console, syslog, SNMP traps; SNMP MIB-II support; System status and session data monitoring; and extensive statistics.

Client Mode and Network Extension Mode

The VPN 3002 works in either of two modes: Client mode or Network Extension mode.

- **Client mode**, also called PAT (Port Address Translation) mode, isolates all devices on the private network from the public network.

  In Client mode, all traffic from the private network appears on the public network with a single source IP address, which is the IP address assigned for tunneled traffic from the central-site VPN Concentrator. The IP addresses of the devices on the VPN 3002 private network are hidden; you can not ping or access a device on the VPN 3002 private network from the central site. Some applications are incompatible with PAT mode.

- **Client Mode with Split Tunneling**

  You always assign the VPN 3002 to a client group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec and PAT are applied to all traffic that travels through the VPN 3002 to networks within the network list for that group.

  Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the assigned IP address of the public interface and also keeps track of these mappings so that it can forward replies to the correct device.

  The network and addresses on the private side of the VPN 3002 are hidden, and cannot be accessed directly.

- **Network Extension mode** allows devices behind the central-site VPN Concentrator to have direct access to devices on the VPN 3002 private network. All nodes on the VPN 3002 private network are uniquely addressable via the tunnel, and only over the tunnel. It also supports applications that use dynamically numbered ports.

  To use Network Extension Mode, you must configure an IP address other than the default for the VPN 3002 private interface, and you must disable PAT mode.

- **Network Extension Mode with Split Tunneling**

  You always assign the VPN 3002 to a client group on the VPN Concentrator. If you enable split tunneling for that group, IPSec operates on all traffic that travels through the VPN 3002 to networks within the network list for that group. PAT does not apply.

  Traffic from the VPN 3002 to any destination other than those within the network list on the central-site Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices on the VPN 3002 private network to the address of the VPN 3002 public interface. Thus the network and addresses on the private side of the VPN 3002 can be accessed directly over the tunnel, but are protected from the Internet, that is, they cannot be accessed directly.

Tunnel Initiation

The VPN 3002 always initiates the tunnel to the central-site VPN Concentrator. The VPN Concentrator cannot initiate a tunnel to a VPN 3002. The VPN 3002 creates only one IPSec tunnel to the VPN Concentrator, in either PAT or Network Extension mode. With split tunneling enabled, it can support multiple unencrypted data streams.

After the tunnel is established between the VPN 3002 and the VPN Concentrator, the VPN Concentrator can initiate data exchange only in Network Extension mode with all traffic travelling through the tunnel. If you want the tunnel to remain up indefinitely, you should configure the VPN 3002 for Network Extension mode and not use split tunneling.

The following table summarizes instances in which the VPN 3002 and the central-site VPN Concentrator can initiate data exchange.

Mode	Tunneling Policy	VPN 3002 Can Send Data First	Central-Site VPN Concentrator Can Send Data First (after VPN 3002 initiates the tunnel)
Client/ PAT	Tunnel everything	Yes	No
Client/ PAT	Split tunneling enabled	Yes	No
Network Extension	Tunnel everything	Yes	Yes
Network Extension	Split tunneling enabled	Yes	No

See the *VPN 3002 Hardware Client Getting Started* manual for

- more information about Client mode and Network Extension mode.
- required settings on the VPN Concentrator to which this VPN 3002 connects.

Management Interfaces

The VPN 3002 offers multiple management interfaces. Each interface provides complete capabilities that you can use to configure, administer, and monitor the device. By default, for security, you cannot manage the device from the public interface.

- The VPN 3002 Hardware Client Manager is an HTML-based interface that lets you manage the system remotely—from the private LAN or through the VPN tunnel—with a standard Web browser using either
  - HTTP connections
  - HTTPS (HTTP over SSL) secure connections
  - XML over HTTPS

- The VPN 3002 Command Line Interface (CLI) is a menu-based interface that you can use with the local system console or remotely—from the private LAN or through the VPN tunnel— using:
  - Telnet connections
  - Telnet over SSL secure connections
  - SSH secure connections
  - XML over SSH

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

> **Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select **Software & Support: Online Technical Support: Software Bug Toolkit** or navigate to http://www.cisco.com/support/bugtools.

Open Caveats

The following problems exist with VPN 3002 Hardware Client, Release 3.5.

- CSCds75601

  The VPN 3002 DHCP server does not restore DHCP leases after the VPN 3002 reboots. DHCP clients must renew their leases to populate the VPN 3002 DHCP server.
- CSCdt08520

  IKE Diffie-Hellman Groups 1 and 7 are supported between the VPN 3000 Concentrator and the VPN 3002 Hardware Client only when digital certificates are in use. Specifically, unless the VPN 3002 Hardware Client uses a digital certificate, only Diffie-Hellman Group 2 is supported.
- CSCdt38841

  The VPN 3002 DHCP server sometimes assigns addresses that are not in sequence, skipping addresses that are free for use.

- CSCdt42421, CSCdu57252

  The Traceroute debugging tool does not work from a device on the private LAN of a VPN 3002.

- CSCdu50355

  When viewing the VPN 3002 ARP table with PPPoE enabled, entries for Interface 12 appear. Interface 12 is currently being used as the PPPoE interface.

- CSCdu52733

  When the route table for a VPN 3002 with PPPoE enabled is displayed on either the CLI or HTML interface, the following route appears in the table. Ignore it.

  ```
  Address        Mask        Next Hop        Int
  0.0.0.0     255.0.0.0      0.0.0.0      public in
  ```

- CSCdu57255

  When the VPN 3002 is configured for 10 Mbps and the duplex mode is configured for auto, the duplex mode may be incorrectly displayed as "half" duplex even though it is running at "full" duplex.

- CSCdv27743

  Using the rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

  The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than 1 certificate with any particular DN.

- CSCdv37212, CSC85594

  If a VPN 3002 uses a DNS name for the connection, the VPN 3002 may be unable to reconnect after a rekey.

- CSCdv50669

  If there are more than 150 networks in a network list used for split tunneling on the central site VPN Concentrator, when a VPN 3002 connects to the VPN Concentrator using this group and attempts to establish an SA to all of the networks within that network list, it may cause a reboot. We recommend that a network list that applies to a VPN 3002 contain 150 or fewer networks.

- CSCdv66367

  The VPN 3002 experiences an exception when the static route, default route, or interface setting is deleted/modified.

- CSCdv69320

  With an active tunnel between a VPN 3002 and VPN Concentrator, occasionally the event `IPSec input- discarding pkt with no NAT Rule` displays. No negative operational issues have been noted when this happens.

- CSCdv72871

  VPN 3002 does not accept a DHCP address when the relay device sets unicast_ DHCPOFFER packet with the BROADCAST flag SET.

- CSCdv85725

  When using Challenge-based authentication such as New PIN mode for SDI, the command-line interface does not present the question or reply text. The workaround is to use the HTML interface.

- CSCdv86086

  The Nexland router has problems with IKE Phase-1 rekeying. When this happens the 3002 tunnel disconnects. Data movement brings up the tunnel again.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

VPN 3002 Documentation

VPN 3002 documentation includes the following:

- The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is online only.
- The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.
- The HTML interface, called the VPN 3002 Hardware Client Manager, includes extensive context-sensitive online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.
- The *VPN 3002 Hardware Client Quick Start* card summarizes information for Quick Configuration. This quick reference card is provided with the VPN 3002, and is also available online. For easiest use, print it on 8 1/2” x 11” paper, in duplex mode. Current customers who obtain version 3.5 software from CCO can also order the 3.5 version of the card from CCO. When ordering the card, use product number DOC-????.
- The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for installing the VPN 3002 and beginning configuration. We suggest that you can affix the label to the VPN 3002 as a ready reference. You can also print a copy of the label from the online version. Current customers who obtain version 3.5 software from CCO can also order the 3.5 version of the label from CCO. When ordering the label, use product number CVPN3002-LABEL-35=.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.