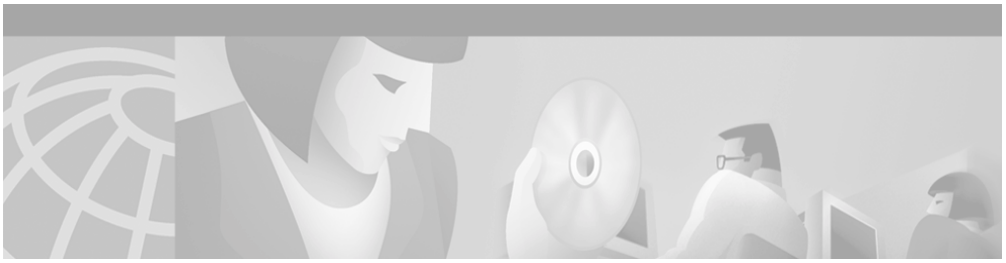

Release Notes for Cisco VPN 3002 Hardware Client Release 3.1

CCO August 20, 2001

Note You can find the most current documentation for the Cisco VPN 3002 on CCO.

These release notes describe the features of the Cisco VPN 3002 Hardware Client and the caveats that apply for Release 3.1. 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 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.
- 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, configure either a default gateway or 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.

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.

Features Summary

The VPN 3002 Hardware Client has the following features:

Hardware Features

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 feature:

- 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

Software Features

The VPN 3002 software includes:

- PPP over Ethernet (PPPoE), which lets a network client interact with service provider equipment, such as a broadband modem, most often xDSL. See the section, “PPPoE” for more information.
- Two operating modes: Client/PAT mode and Network Extension mode. See the section, “Modes” for more information.

- Multiple management interfaces: HTML and command-line interface.
- An auto-update feature that lets you upgrade software for multiple hardware clients from a single, central-site location.
- IPSec as the tunneling protocol.
- UDP NAT/FW Transparent IPSec, which enables secure transmission between the VPN 3002 Hardware Client and the central-site Concentrator through a device, such as a firewall, that is performing Network Address Translation (NAT). See the section, "UDP NAT/FW Transparent IPSec" for more information.
- Two encryption algorithms: 56-bit DES (Data Encryption Standard) and 168-bit Triple DES.
- 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, using Internet Key Exchange (IKE) (formerly called ISAKMP/Oakley) with Diffie-Hellman key technique.
- Network addressing support using DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) client and server.
- Support for multiple certificate authorities: Baltimore, Entrust, Microsoft Windows 2000, Netscape, RSA Keon, and VeriSign.
- System administration features: session monitoring and management, software image update, system reset and reboot, PING capability, configurable system administrator profiles, and digital certificate management.
- Monitoring capabilities, such as: event logging and notification via system console, syslog, SNMP traps; SNMP MIB-II support; System status and session data monitoring; and extensive statistics.

Modes

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 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 behind the central-site Concentrator.

  Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site 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 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 central-site 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 behind the central-site Concentrator. PAT does not apply.

Traffic from the VPN 3002 to any other destination 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 Concentrator. The central-site Concentrator cannot initiate a tunnel to a VPN 3002. The VPN 3002 creates only one IPSec tunnel to the central-site 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 central-site Concentrator, the central-site 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 Concentrator can initiate data exchange.

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

- The VPN 3002 Command Line Interface (CLI) is a menu- and command-line 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

The amount of time remaining until the current IP address lease expires, shown as HH:MM:SS.

PPPoE

PPPoE lets a network client interact with a service provider's equipment, such as a broadband modem—most often xDSL—to achieve access to high-speed data networks. It relies on the Ethernet and PPP standards. It uses an authentication strategy that includes a username and password to create a PPPoE session from the VPN 3002 to your ISP Access Concentrator.

PPPoE is a VPN 3002 feature, transparent to the central-site Concentrator to which the VPN 3002 connects. To use PPPoE, for the VPN 3002 public interface you must:

- Enable PPPoE.
- Supply a username and password.

UDP NAT/FW Transparent IPSec

UDP NAT/FW Transparent IPSec enables secure transmission between the VPN 3002 Hardware Client and the central-site Concentrator through a device, such as a firewall, that is performing Network Address Translation (NAT).

Using this feature encapsulates encrypted data traffic within UDP packets. The VPN 3002 also sends keepalives frequently, ensuring that the mappings on the NAT device are kept active.

While you do not have to configure this feature on the VPN 3002, the following requirements do apply. To use IPSec through NAT:

- You must upgrade **both** the central-site Concentrator and the VPN 3002 to Release 3.0.2 or higher.

- The central-site group on the Concentrator must be configured to support it. For an example, refer to the VPN Concentrator Manager, Configuration | User Management | Groups | IPSec tab (see *VPN 3000 Concentrator Series Reference* volumes or refer to the VPN Concentrator Manager Help).
- Cisco does not support a topology with multiple VPN 3002s behind one NAT device.

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 3.1.

- 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.

- CSCdt21080

  Unable to unlock a locked configuration

  If you are managing a device and do not log out properly, the configuration file is locked by any other IP Address of the managing device until that session expires.

  For a VPN 30xx Concentrator, you can physically log out this admin user, but with a VPN 3002, the problem persists until the session expires (the default is 10 minutes) or you reboot the unit.

- CSCdt28156

  Using Port Address Translation (PAT) and non-compliant FTP shareware applications can cause a problem. For example, with both Sambar and TSoft FTP shareware, the Server changes the source port to something other than "20" (which is the FTP-Data port outlined in the RFC). To work around this problem, use passive mode FTP instead of active.

- CSCdt38841

  The VPN 3002 DHCP server may at times assign addresses that are not in sequence, skipping addresses that are free for use.

- CSCdt42173

  The VPN Concentrator family of products does not support SSH connections from TeraTerm SSH version: TTSSH v1.2/TTPRO v2.3. If you plan to use SSH from TeraTerm, and are currently running this version, visit the following site and upgrade your SSH software: http://www.zip.com.au/~roca/ttssh.html

- CSCdt42408

  The MS Exchange/Outlook auto-update feature doesn't work in Client (PAT) mode. There is an open Microsoft bug for this problem.

- CSCdt42421, CSCdu57252

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

- CSCdt48908

  When changing IP addresses (from static to DHCP mode and vice-versa) on the VPN 3002 public interface, data starts passing approximately 30 seconds after the tunnel to the central-site VPN 3000 has been established.

- CSCdt49326, CSCdu57255

  When the VPN 3002 is configured for 10 Mbps and the duplex mode is configured for auto, the duplex mode made be incorrectly displayed in the Monitor | Statistics | MIB II | Interfaces | Ethernet screen as "half" duplex even though it is running at "full" duplex.

- CSCdu40803

  The 3002 may reboot after several hours of failed authentication attempts during PPPoE negotiation. Make sure the correct name and password are configured.

- CSCdu50355

  When you view 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 two routes appear in the table. Ignore them.

Address	Mask	Next Hop	Int
0.0.0.0	0.0.0.0	133.3.0.40	12
0.0.0.0	255.0.0.0	0.0.0.0	public in

- CSCdu63947

  When the VPN 3002 initially boots with PPPoE enabled, it generates an ARP request for address 0.0.0.1. This is the temporary IP address for the physical public interface.

- CSCdu66046

  On a VPN 3002 configured for PAT mode, after an IPSec rekey occurs, the Assigned IP Address field does not display on the System Status window.

Resolved Caveats

The following problems have been resolved as of version 3.0.1.

- CSCdt42413

  We have added more information, including port numbers and protocol, to the event messages that are logged when packets that come in over the VPN 3002 tunnel are rejected because there is no applicable NAT rule.

- CSCdt48863

  If a VPN 3002 has been configured to acquire a public address via DHCP, and is re-configured to have a static IP address, the system now automatically disables the DHCP client.

- CSCdt64686

  RIP listen is now disabled by default on the VPN 3002 Private interface.

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 3.1 software from CCO can also order the 3.1 version of the card from CCO. When ordering the card, use product number DOC-7812273=.
- 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 3.1 software from CCO can also order the 3.1 version of the label from CCO. When ordering the label, use product number CVPN3002-LABEL-31=.

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.