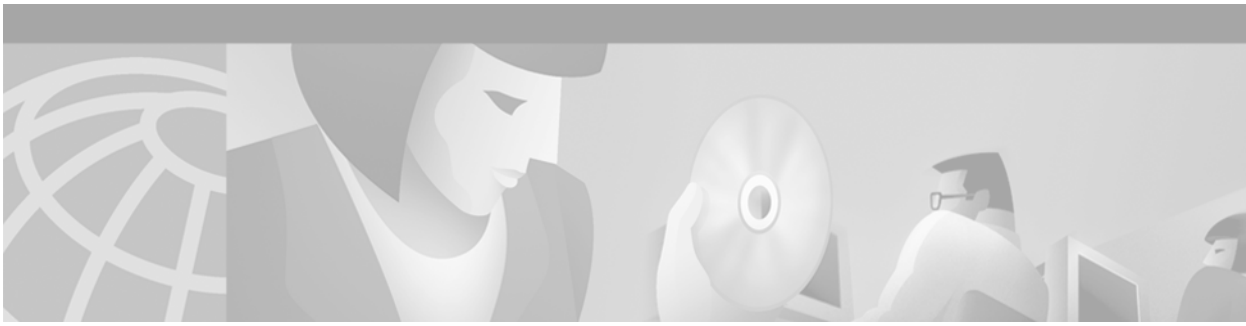

Release Notes for the Cisco VPN 5000 Concentrator Software Version 5.2.23.0004

August 6, 2002

These release notes provide information about the Cisco VPN 5000 concentrator software Version 5.2.23.0004. These release notes are periodically updated to describe new features, caveats that were fixed from the previous releases, closed caveats, and documentation updates.

Contents

These release notes contain the following sections:

- New Features, page 2
- Important Notes, page 7
- Hardware Supported, page 8
- Interoperability, page 9
- Caveats Fixed, page 9
- Closed Caveats, page 19
- Obtaining Documentation, page 25
- Obtaining Technical Assistance, page 26

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

New Features

The following sections describe new features, including new keywords, for each release.

New Features in Version 5.2.23.0003

This section describes the new features in the Cisco VPN 5000 concentrator software Version 5.2.23.0003.

RADIUS Service Type Keyword

The following keyword was added to the **Radius** section:

ServiceType = {On | Off}	• **On**—Includes service type 8 (Authenticate-Only) in Access-Request packets. Older Livingston RADIUS services required this service type when using passthrough mode with SecurID. **Note** This setting was the default in previous releases. The default was changed to **Off** in this release because some newer RADIUS servers fail when the service type is set to Authenticate-Only. • **Off** (Default)—Does not include a service type in Access-Request packets. Most older RADIUS servers ignore the service type, but newer servers can fail if the service type is set to Authenticate-Only. These same servers succeed when no service type is included.

New Features in Version 5.2.23.0001

The following section describes the new**VPN Group** section **ExcludeIPNet** keyword.

Exclusion of Networks from VPN 5000 Client Tunnels

You can now exclude certain networks from being tunneled by VPN 5000 client Version 5.2 or later. Formerly, you identified the networks you wanted to tunnel on the concentrator using the **VPN Group** section **IPNet** keyword. Each **IPNet** is tunneled by the connected client. By using the new **VPN Group** section **ExcludeIPNet** keyword, you can specify networks you do not want to tunnel even though they are identified as part of an **IPNet** network. For example, you can tunnel all networks (**IPNet = 0.0.0.0/0**) except for 192.168.1.0/24 (**ExcludeIPNet = 192.168.1.0/24**). Without **ExcludeIPNet**, you must identify a large number of **IPNet** keywords to approximate the same functionality.

See the following information about the **VPN Group** section **ExcludeIPNet** keyword:

ExcludeIPNet = *IP_Address/bits*	**Client Version:** VPN 5000 client Version 5.2 and later **Multi-keyword:** To exclude multiple networks, enter this keyword up to 32 times for 32 networks. A network that you do not want remote clients to reach through the tunnel. Traffic to this network is managed by the local ISP (similar to the **ExcludeLocalLAN** keyword). Typically, this network is part of an **IPNet** network. **ExcludeIPNet** networks take precedence over **IPNet** networks when the client determines whether to tunnel a packet. To exclude tunneling to a single host, specify the *bits* as 32. If you use client Version 5.1 or earlier with a concentrator on which you set the **ExcludeIPNet** keyword, the client displays an error.

ExcludeIPNet Examples

The following example shows how to tunnel all networks except 192.168.1.0/24:

```
[ VPN Group "isakmp" ]
Transform = esp(sha)
IPNet = 0.0.0.0/0
ExcludeIPNet = 192.168.1.0/24
MaxConnections = 4
StartIPAddress = 10.7.10.128
```

The following example shows how to tunnel all traffic to 10.1.0.0/16 except for 10.1.1.0/24:

```
[ VPN Group "isakmp" ]
Transform = esp(sha)
IPNet  = 10.1.0.0/16
ExcludeIPNet = 10.1.1.0/24
MaxConnections = 254
LocalIPNet = 10.2.1.0/24
```

New Features in Version 5.2.22

The following section describes the new **certificate cg** command.

Transfer Root Certificate and Private Key Between Certificate Generators

If you are using the VPN 5000 concentrator as a certificate generator (CG), and you need to replace the system, you can use the new **certificate cg** command to transfer the root certificate and private key bundle to a new CG or to a file server for archiving purposes. Generating server certificates can be time consuming, and this command allows you to keep any existing server certificates if the CG fails. Use the following syntax:

certificate cg {export | import} *password*

Usage Guidelines

We recommend running this command on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Options

export | **import**	• **export**—Displays the encrypted (see the *password* below) root certificate and private key bundle in PKCS#12 format on the CG console. You can then copy the bundle to a new CG using the **import** option. When you select the text on the console, be sure to include a carriage return after the last line. Selecting the last carriage return might require you to select the area in front of the prompt that follows the text. The CG still has the root certificate and private key installed after you export a copy. • **import**—Allows you to paste a root certificate and private key bundle from the clipboard to the new CG. The system prompts you to paste the bundle. Paste the bundle at the prompt, add a period (**.**) on a separate line after the bundle, and press **Enter**. If the system already has a root certificate, it is overwritten by this new one.
password	**Length:** 50 characters The password to encrypt the root certificate and private key bundle when you use the **export** option. The same password decrypts the bundle when you use the **import** option.

Examples

The following examples how how to export and import a root certificate and private key bundle.

Exporting a Cerificate Bundle

The following steps show how to use the **certificate cg export** command:

1. On the original CG, enter:

```
orig_cg# certificate cg export kahuna
```

2. The console displays the root certificate and private key bundle in PKCS#12 format:

```
Successful

-----BEGIN PKCS12-----
MIID7QIBAzCABgkqhkiG9w0BBwGggASCA6QwggOgMIAGCSqGSIb3DQEHBqCAMIIB
rAIBADCCAaUGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEGMA4ECKmsDZ+H17J9AgII
AICCAXh2rRTQEg8507Af1I3n7JQ0sYOFSfZY8QjsxEJpG0CPC5/op7AeoOiOdxqt
j2WCBtKJldom1FDOLQYeHk9Y9RUo8BkVFs8r3ZWm/bhLDvuL3m1v2qe1Uvr4Ha6+
lCNUTaOWyJefAGgYbMYZFsBY3LWuGwzmXU3km1b/DVkcY+tPEERn0XaFgavgl2xH
kquBryxnrEBepoNfZJf7KLlcYT7lj3cAHYXPA0TJDTvLu9Za30cWtz53YHeUr7MU
QX9Unek2//halTB7frZYu2V8njoeqIQFNMcZmtb2xPFugAjNXgXkQHNziRYkuW5A
sj5EAweIcpgSrXEMX5fz3djZSytKjktmN0LU1WNVgt9csUGQPK3XDmLN4EojdBOJ
LtS0uR6GXduRbXNKCiwgzaDztvajacqgppzkc+MZ52+MftS3orE3ltk/A/3tSAlm
qYAbw/6IbnA4HkQ8IktFQryYf/5O04BbiRNOxApZyHD6vjHBP0vCo1GxYK1BAAAA
ADCABgkqhkiG9w0BBwGggASCAcYwggHCMIIBvgYLKoZIhvcNAQwKAQKgggGGMIIB
gjAcBgoqhkiG9w0BDAEDMA4ECJU6PZuUJtwzAgIIAASCAWB2XZvTeZ2jBfCvgTu+
DJgNm/rjt6TZV4Q7P5g3j2k2MitQYpPayeyqTMVCFWqSUH59eBc9HJ734aenkd2A
tbPf+/gm+ZQ4G4Qvpdtml/haxYgd5B8RgUGt/YEcyv0WdFdA+yuijYC3eqWfgaaa
lELHjFX7kAnUGdVtMpe2gTgN1W89thsCDbR7//Ff43BEemE81N4O9EpDbqpz4DP/
4fSIB9nv4rLpNQv6Q+DYozkpJ9flqpkzjR3HVTXwaOY2c+zpccCyLX4ys6aMSomS
JNeFQBhoGqtq9dVKnfwTcxHjKGo06hT7wNCoJNi9Lgt9VEWyPVLTEBI7gpMZyE8S
07A0f7GmVLNsaklAhaNoFJWhkbux2px7D593X+WHqIaGSWA5q+ILyww2zFuh1ANz
m5KDcHCI3m0RnooLCuGPIrP390oyFjlb9v763ApaF+guSMvfD4YGROHXg/PvIY2M
UZTRMSUwIwYJKoZIhvcNAQkVMRYEFH2Jol4uCF1co0XgcEAQ1zQT1pLmAAAAAAAA
```

```
AAAwLTAhMAkGBSsOAwIaBQAEFK8iq4HQUYmhGKZKimGIjY3+KzA5BAh9H5wSyh0g
Jg==
-----END PKCS12-----
orig_cg#
```

3. Copy the bundle to the clipboard or to a text editor. Make sure to include the last carriage return before the prompt.

Importing a Certificate Bundle

The following steps show how to use the **certificate cg import** command on the new CG:

1. Enable the CG feature on the new CG by setting the **Certificates** section **CertificateGenerator** keyword to **On**, and use the **save** command to write and apply the configuration change.
2. At the prompt, enter:

```
new_cg# certificate cg import kahuna
```

3. You are prompted to paste the bundle:

```
Begin Pasting Certificate Now
To terminate input, enter a . on a line all by itself.

-----BEGIN PKCS12-----
MIID7QIBAzCABgkqhkiG9w0BBwGggASCA6QwggOgMIAGCSqGSIb3DQEHBqCAMIIB
rAIBADCCAaUGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEGMA4ECKmsDZ+H17J9AgII
AICCAXh2rRTQEg8507Af1I3n7JQ0sYOFSfZY8QjsxEJpG0CPC5/op7AeoOiOdxqt
j2WCBtKJldom1FDOLQYeHk9Y9RUo8BkVFs8r3ZWm/bhLDvuL3m1v2qe1Uvr4Ha6+
lCNUTaOWyJefAGgYbMYZFsBY3LWuGwzmXU3km1b/DVkcY+tPEERn0XaFgavgl2xH
kquBryxnrEBepoNfZJf7KLlcYT7lj3cAHYXPA0TJDTvLu9Za30cWtz53YHeUr7MU
QX9Unek2//halTB7frZYu2V8njoeqIQFNMcZmtb2xPFugAjNXgXkQHNziRYkuW5A
sj5EAweIcpgSrXEMX5fz3djZSytKjktmN0LU1WNVgt9csUGQPK3XDmLN4EojdBOJ
LtS0uR6GXduRbXNKCiwgzaDztvajacqgppzkc+MZ52+MftS3orE3ltk/A/3tSAlm
qYAbw/6IbnA4HkQ8IktFQryYf/5O04BbiRNOxApZyHD6vjHBP0vCo1GxYK1BAAAA
ADCABgkqhkiG9w0BBwGggASCAcYwggHCMIIBvgYLKoZIhvcNAQwKAQKgggGGMIIB
gjAcBgoqhkiG9w0BDAEDMA4ECJU6PZuUJtwzAgIIAASCAWB2XZvTeZ2jBfCvgTu+
DJgNm/rjt6TZV4Q7P5g3j2k2MitQYpPayeyqTMVCFWqSUH59eBc9HJ734aenkd2A
tbPf+/gm+ZQ4G4Qvpdtml/haxYgd5B8RgUGt/YEcyv0WdFdA+yuijYC3eqWfgaaa
lELHjFX7kAnUGdVtMpe2gTgN1W89thsCDbR7//Ff43BEemE81N4O9EpDbqpz4DP/
4fSIB9nv4rLpNQv6Q+DYozkpJ9flqpkzjR3HVTXwaOY2c+zpccCyLX4ys6aMSomS
JNeFQBhoGqtq9dVKnfwTcxHjKGo06hT7wNCoJNi9Lgt9VEWyPVLTEBI7gpMZyE8S
07A0f7GmVLNsaklAhaNoFJWhkbux2px7D593X+WHqIaGSWA5q+ILyww2zFuh1ANz
m5KDcHCI3m0RnooLCuGPIrP390oyFjlb9v763ApaF+guSMvfD4YGROHXg/PvIY2M
UZTRMSUwIwYJKoZIhvcNAQkVMRYEFH2Jol4uCF1co0XgcEAQ1zQT1pLmAAAAAAAA
AAAwLTAhMAkGBSsOAwIaBQAEFK8iq4HQUYmhGKZKimGIjY3+KzA5BAh9H5wSyh0g
Jg==
-----END PKCS12-----
.
PKCS12 Import Successful
new_cg#
```

4. You can now generate a server certificate using the **certificate generate server** command.

New Features in Version 5.2.21

The following section describes the **VPN Group** section **AbsoluteTimeout** keyword.

VPN Client Timeout Keyword

The following new keyword in the **VPN Group** section times out a VPN client.

AbsoluteTimeout = *Seconds*	**Values:** 0 to 2,592,000 seconds (30 days) **Default:** 0 (no timeout) The maximum amount of time a client can stay connected, regardless of client activity. When the **AbsoluteTimeout** value is reached, the concentrator disconnects the client. The client must reconnect and begin a new session.

New Features in Version 5.2.20

The following section describes the new **General** section **NATTransport** keyword.

Configurable NAT Transparency Port

The following keyword in the **General** section allows you to configure one or more TCP ports for NAT transparency.

NATTransport = *Number*	**Values:** 0 to 65536 **Default:** 80 **Limitations:** Nondefault values sre only valid for VPN 5000 client Version 5.1 or later **Multikeyword:** You can enter this keyword multiple times to support multiple port numbers. Sets the TCP port number used to encapsulate VPN packets. VPN packets consist of ESP packets and UDP packets. This keyword does not support the AH transform (see the **VPN Group** section **Transform** keyword). NAT devices that do not use 1:1 IP address mapping cannot forward ESP packets successfully, because ESP packets do not include a unique port number. TCP packets can include a unique port number. If your firewall blocks ESP or UDP packets, this parameter allows you to successfully maintain a client connection by encapsulating the packets in a TCP packet. If you are using clients earlier than Version 5.1, be sure to set one instance of this keyword to 80, which is the port supported by older clients.

New Features in Version 5.2.14

Table 1 lists new software features that were incorporated after Compatible Systems IntraPort software Version 5.1.x was introduced. IntraPort servers are now called the Cisco VPN 5000 concentrator series.

Table 1 VPN 5000 Software New Features

Feature	Description
Server-side certificates and certificate generation	Allows AXENT Defender, SecurID, and RADIUS to use server-side certificates to authenticate clients.
No differentiation between supported numbers of client tunnels and LAN-to-LAN tunnels	Allows you to combine tunnels of any type to reach the maximum number of tunnels supported.
LAN-to-LAN tunnel rekeying and perfect forward secrecy (PFS)	Increases the security of the tunnel through: • Rekeying, which forces the tunnel to periodically be reestablished with a new key. • PFS, which specifies that each time the concentrator computes encryption or authentication keys, it includes a new Diffie-Hellman Key Exchange. Both techniques greatly increase the difficulty of finding the session keys used to encrypt a VPN session.
Dynamic responder for LAN-to-LAN tunnels	Allows you to configure a concentrator as a dynamic responder to allow tunnels to any remote peer, without having to configure the concentrator for communication with each individual peer.
New or improved VPN management commands	• **show vpn** command provides extensive displays to help troubleshoot and maintain VPN tunnels. • **reset vpn** command terminates VPN tunnels. • **vpn cutoff** command stops new connections.

Important Notes

- The **apply** command was removed from software Version 5.2.22 because the results of **apply** were not consistent across all sections. To apply configuration changes, use the **save** command (to write changes to Flash memory and reboot immediately) or use the **write** command followed by the **boot** command when you are ready to reboot.
- The **VPN Group** section **BackupServer** command is no longer supported because its function was meant for concentrators that support several dozen clients, not the thousands of clients currently supported.
- For full OSPF functionality, upgrade to Version 6.0. Version 5.2 includes many OSPF caveats that are not present in Version 6.0.

Hardware Supported

Table 2 lists the hardware and software builds supported for concentrator software Version 5.2.22.

Table 2 Supported Hardware for Software Version 5.2.22

Model	Software Build
IntraPort 2[1]	vpn-intraport-2-*x.x.x*[*.xxxx*][2]-[3][3]des.dld
IntraPort 2+[1]	vpn-intraport-2plus-*x.x.x*[*.xxxx*]-[3]des.dld
VPN 5001	vpn-5001-*x.x.x*[*.xxxx*]-[3]des.dld
IntraPort Carrier and Enterprise[1], VPN 5002 and 5008	vpn-5002-5008-*x.x.x*[*.xxxx*]-[3]des.dld

1. Compatible Systems legacy platforms.
2. *x.x.x*[*.xxxx*] is the software version, for example, 5.2.23 or 5.2.23.0003.
3. U.S. builds include 3DES; export builds include DES. The filename reflects the encryption level.

Upgrading the IntraPort 2 and 2+ Servers to Cisco VPN 5001 Software

For the latest software releases and caveat fixes, you need to upgrade the IntraPort 2 or 2+ servers to a Cisco VPN 5001 software build. The IntraPort 2 and 2+ servers function the same as the VPN 5001 concentrator except for the number of tunnels supported. Table 3 lists the tunnels supported for each platform.

For information about configuring and upgrading the IntraPort 2 and 2+, use the information about the VPN 5001 concentrator in the *Cisco VPN 5000 Software Configuration Guide*.

Table 3 Tunnels Supported for the VPN 5001 and IntraPort 2 and 2+

Model	Tunnels
VPN 5001 concentrator	1500
IntraPort 2+	500
IntraPort 2	64

Upgrading the IntraPort Carrier and Enterprise Servers to Cisco VPN 5002 and 5008 Software

To receive the latest software releases and caveat fixes, you must upgrade the IntraPort Carrier and Enterprise servers to a Cisco VPN 5002 and 5008 software build. The IntraPort Carrier and Enterprise servers function the same as the VPN 5002 or 5008 concentrators. For information about configuring the IntraPort Carrier and Enterprise servers, see the VPN 5002 and VPN 5008 information in the *Cisco VPN 5002 and 5008 Software Configuration Guide*. The Carrier and Enterprise servers use the same software build as the VPN 5002 and VPN 5008 concentrators.

You can upgrade the carrier server according to the *Cisco VPN 5000 Software Configuration Guide* (the same as a Cisco VPN 5002 or 5008 concentrator). See the following steps to upgrade an enterprise server.

Note You must perform this procedure the first time you upgrade an enterprise server to Version 5.2.x or later. After you perform the upgrade, you can use the normal procedure to load software.

Step 1 As a precaution, save the configuration by using TFTP according to the *Cisco VPN 5000 Software Configuration Guide.*

This procedure preserves and uses the configuration already in the concentrator. To copy the configuration back to the concentrator at the end of this procedure, copy it using the following filename:

vpn5002_8.cfg

Step 2 On the card in slot 0, attach a console to the console port.

Step 3 On the card in slot 0, set the test switch to position 3.

Step 4 Restart the concentrator.

Step 5 At the console prompt, enter:

setip *address mask* [*gateway*]

Where:

- *address* is the IP address of the port in slot 0.
- *mask* is the subnet mask.
- *gateway* is the default gateway.

Step 6 Set the test switch back to 0.

Step 7 Download the new vpn-5002-5008-*x.x.x*-[3]des.dld software using TFTP or the VPN 5000 Manager.

After you perform the download, the concentrator reboots using the new software. The software then propagates to the other cards in the chassis.

Interoperability

The VPN 5000 concentrator series can establish LAN-to-LAN tunnels with other Cisco products that support:

- IPSec DES or 3DES
- Cisco IOS Release 12.1(1)T or Release 12.1(2)

Caveats Fixed

The following sections list caveats that were fixed in each release.

Caveats Fixed in Version 5.2.23.0004

This section lists caveats fixed with VPN 5000 concentrator software Version 5.2.23.0004.

- CSCdx82483

  Formerly, if you used a RADIUS server to authenticate client connections using the PAP or Challenge (a hybrid of PAP) challenge type, and if validation failed the first time, then the validation retry request that the VPN 5000 concentrator sent to the RADIUS server did not encrypt the user

password field; the concentrator sent the password as clear text. Connections using CHAP are not affected by this vulnerability. This problem is fixed in Version 5.2.23.0004. See http://www.cisco.com/warp/public/707/vpn5k-radius-pap-vuln-pub.shtml for more information.

Caveats Fixed in Version 5.2.23.0003

This section lists caveats fixed with VPN 5000 concentrator software Version 5.2.23.0003.

- CSCdu78571

  The concentrator now allows you to exclude the service type from RADIUS Access-Request packets when you use the **Radius** section **ServiceType** = {**On** | **Off**} keyword. Formerly, the concentrator always included service type 8 (Authenticate-Only) in Access-Request packets. Older Livingston RADIUS services required this service type when using passthrough mode with SecurID. Most older RADIUS servers ignore the service type, but newer servers can fail if the service type is set to Authenticate-Only. These same servers succeed when no service type is included.

- CSCdx16385

  If the concentrator loses connectivity to the RADIUS server, the concentrator now starts sending Access-Request packets when connectivity is restored. Formerly, in some heavy traffic situations, the concentrator did not resume RADIUS operations.

- CSCdx03698

  Traceroute now works through a Mac OS X or Solaris tunnel when you use NAT transparency. Formerly, the concentrator did not recalculate the ICMP checksum after NAT processing, and the traceroute would fail.

- CSCdx07575

  RADIUS passwords are no longer truncated to 15 characters when using PAP authentication. The limit is now 30 characters.

- CSCdx10541

  The PPTP feature is no longer available in the command line interface. This feature was never supported, but was not removed from the software until this release.

Caveats Fixed in Version 5.2.23.0001

- CSCdr87519

  The concentrator now allows you to exclude a network from being tunneled by the VPN 5000 client Version 5.1 and later. See the "New Features in Version 5.2.23.0001" section on page 2 for more information about the **VPN Group** section **ExcludeIPNet** keyword.

- CSCdw45324

  The concentrator no longer restarts after you upgrade to Version 5.2.22. This restart event was related to a NATted FTP port command.

Caveats Fixed in Version 5.2.22

This section lists caveats fixed in software Version 5.2.22.

- CSCco00848

  When the VPN 5000 concentrator is running AppleTalk over a LAN-to-LAN tunnel, duplicate directly connected routes no longer randomly appear in the routing table for one or both ends of the tunnel, and no longer disrupt AppleTalk routing for the tunnel.

- CSCds59954

  The concentrator no longer reports an erroneous value for the RADIUS authentication attribute number 5, the NAS-port. Formerly, Access-Request packets sent by the concentrator to the RADIUS server contained a value for the NAS-Port that was greater than the maximum value specified by RFC 2138. This value interrupted a RADIUS server's ability to perform accounting.

- CSCds66315

  The concentrator no longer loses memory for every VPN client reconnection to cards in slots 1 through 7 (this problem did not occur for connections to slot 0). Upon reconnect, the previously attached memory was not reused or given back to the operating system.

- CSCdt07584

  When you use the **vpn tunnel down** command on a GRE tunnel, the **show vpn partner** command no longer shows the tunnel as active.

- CSCdt46387

  When you use the Linux VPN 5000 client, active FTP sessions no longer lock up.

- CSCdt62717

  The concentrator no longer allows the successful prediction of TCP Initial Sequence Numbers. True hardware random number generation is now used.

- CSCdt81839

  Version 5.x of the Linux and Solaris VPN 5000 client no longer fail when they use a certificate for authentication. Formerly, the concentrator occasionally failed to authenticate clients who used certificates. This condition was also experienced when the **IKE Policy** section **Protection = SHA_3DES_G1** and the **VPN Group** section **Transform = AH(MD5)+ESP(MD5,DES)**.

- CSCdt96436

  The concentrator now sends an SNMP trap correctly.

- CSCdu34359

  The concentrator no longer stops accepting VPN 5000 client connections after 200 connections are established. Formerly, the **show vpn statistics** command showed a large number of connections in negotiation.

- CSCdu34720

  The VPN 5008 concentrator no longer restarts after a random amount of time with a reset event that contains the following message:

  ```
  EXCEPTION: Data Access Memory Abort
  ```

- CSCdu38969

  The concentrator no longer restarts when you perform a ping.

- CSCdu49603

  The concentrator can now successfully pass traffic through a NAT device configured to pass through IPSec traffic. Formerly, although a client could connect to the concentrator behind the NAT device, no IPSec traffic could pass through.

- CSCdu54980

  The first 1 MB of memory on the concentrator is now protected from accidental writes.

- CSCdv06547

  On a VPN5002 or VPN5008 concentrator, after rebooting the device, the console no longer repeatedly reports this message:

```
Attempting to contact other IOPs...
 Attempting to contact other IOPs...
 Attempting to contact other IOPs...
 Attempting to contact other IOPs...
 Attempting to contact other IOPs...
 Attempting to contact other IOPs...
 Still waiting for interfaces on IOP:1
```

  This message identifies that the route processor card in slot 0 was unable to contact one or more other cards.

  Note If you never get the system out of this loop (either by restarting or reseating the card), you must manually load the new software on cards in slots 1 through 7. Normally, when you load new software to slot 0, the software propagates to all other slots. This caveat, however, stops the software from loading on other cards. To load the software directly on a card, set that card's test switch to 3, and follow the instructions in the *Cisco VPN 5000 Concentrator Software Configuration Guide* to download software over a console connection using XModem.

- CSCdv12861

  When a concentrator has a server certificate installed, and the Windows VPN 5000 client Version 5.0.x or 5.1.x connects using a root certificate (Hybrid mode), the RADIUS password prompt is no longer delayed (in excess of 9 seconds).

- CSCdv15501

  In certain high-traffic conditions (for example, in excess of 100 Mbps of 68- or 128-byte packets), the concentrator no longer restarts.

- CSCdv22791

  A client can now connect to the cards in slots 1 through 7, and not just slot 0. Formerly, when a client tried to connect to slot 1, the following debug-level message appeared on the console:

```
IKE WARNING: Variable-length attribute (type 0) found, not processed
```

- CSCdv28869

  The concentrator acting as a certificate generator (CG) can now transfer a root certificate and private key to a new CG. See the "New Features in Version 5.2.22" section on page 3 for more information.

- CSCdv35140

  When you enter the **vpn tunnel down** *vpn_number* command for tunnels on slots 1 through 7, but fail to identify the slot number in *vpn_number*, the concentrator no longer restarts.

- CSCdv46111

  The concentrator no longer receives a UDP packet with an invalid length (for example, an IKE packet). Under rare circumstances, this packet caused the concentrator to restart.

- CSCdv47470

  The concentrator now forwards all IPX requests and replies to the VPN 5000 client, so that login sessions are complete and do not result in timeouts.

- CSCdv56959

  The concentrator now accepts the correct number of VPN users when they use SecurID. Formerly, when a client entered a password that was too short, and a backup SecurID server was configured, the concentrator did not release the memory for the failed connection on the backup server.

- CSCdv60217

  The **vpn tunnel down** command, when entered on a responder connected to another VPN 5000 concentrator, now deletes the tunnel. A concentrator is a responder when you set the **Tunnel Partner** section **KeyManage** keyword to **Respond** or **Auto**; the **Auto** setting automatically sets one concentrator as a responder and one as an initiator. Initiators and dynamic responders already delete the tunnel. Previously, the VPN 5000 initiator automatically brought the tunnel back up within several minutes because the tunnel was not deleted. To bring the tunnel back up now, you must enter the **vpn tunnel up** command on the initiator. Tunnels to Cisco IOS devices are not affected by the tunnel deletion, because they use dynamic tunnel establishment and can re-establish the tunnel when traffic requires it.

- CSCdv68285

  When a VPN 5002 or VPN 5008 concentrator produces a restart event, the restart event now contains backtrace information. Formerly, under some conditions, the following message appeared:

  ```
  Frame pointer out of range!
  ```

- CSCdv70753

  The **show ip route** command no longer causes the concentrator to restart if you enter it after you enter the **vpn tunnel down** command several times.

- CSCdv71366

  The **show os dump** *address* command no longer causes a restart if you enter too many characters for the *address*.

- CSCdv74044

  The **apply** command no longer causes system instability, because the **apply** command is no longer supported.

- CSCdv90469

  The **show appletalk routing** command no longer causes the concentrator to reboot.

- CSCdw04995

  A concentrator configured as a certificate generator (CG) now approves certificate requests successfully. Previously, the CG periodically failed to approve a request and had to be rebooted before succeeding.

- CSCdw13431

  The concentrator no longer locks up after the following log message appears:

  ```
  S_BAD_HASH_CALC
  ```

Caveats Fixed in Version 5.2.21

This section lists caveats fixed in software Version 5.2.21.

- CSCdt46196

  If you use the **show vpn hardware verbose** command on a VPN 5002 or 5008 concentrator, this action no longer shows statistics and restarts the concentrator.

- CSCdu08295

  The concentrator no longer drops packets due to a large amount of traffic. Previously, when VPN traffic reached a level that the device could not match, the traffic in one direction began to drop until all traffic in that direction was lost.

- CSCdu43158

  When you use the VPN 5000 client with Novell's Client 32, an error message no longer appears when you log in to the Novell server and try to connect to the directory structure.

- CSCdu44498

  When you issue the **show vpn users verbose** command, the IPX net number now displays correctly.

- CSCdu47160

  When a VPN client is terminated on slot 1, the concentrator now passes IP traffic.

Caveats Fixed in Version 5.2.20

This section lists caveats fixed in software Version 5.2.20.

- CSCco00847, CSCdr52146

  In VPN 5000 client Versions 5.1.x or later, you now have the capability to set the TCP port number used to encapsulate VPN packets. Use the **NATTransport** keyword in the **General** section.

- CSCdr95270

  If a responder tunnel is configured to have G2 protection, a subsequent tunnel configured to have G1 protection can now be opened successfully.

- CSCds52787

  If the unsupported **PFS** keyword in the **VPN Group** section is inadvertently set to a setting other than **Off**, VPN 5000 client Versions 4.2.x or earlier are now able to pass traffic across the VPN link.

- CSCds68059, CSCdt36092

  The concentrator no longer restarts during a client connection attempt if it is configured with no users in the **VPN Users** section.

- CSCds87292

  Failed VPN 5000 client connections now free resources correctly in the concentrator. Previously, client failures caused the **vpn summary** command to show connection attempts that remained in the "in negotiation" state when using concentrator software Version 5.2.19 and a VPN 5000 client Version 4.2.18 configured with hybrid mode certificates and SecurID authentication.

- CSCdt25612

  A VPN 5000 client configured to use RADIUS authentication to AXENT Defender using CiscoSecure ACS now works correctly when you initiate a connection to a VPN 5008 concentrator.

- CSCdt28673

  An internal timing condition no longer causes intermittent restarts on the concentrator.

- CSCdt42127

  IP filters assigned to a VPN port now filter packets correctly.

- CSCdt47815

  A VPN 5000 client can now connect to a concentrator behind a PIX using NAT transparency mode. Previously, the connection could not be established because previously connected VPN client connections did not correctly disconnect.

- CSCdt53391

  When you use the **show snmp config** command in enabled mode, the concentrator no longer restarts.

- CSCdt65567

  When client connections do not complete authentication, connection resources are no longer held, causing the tally for sessions “in negotiation” to increase.

- CSCdu18675

  Users in the **VPN Users** section who repeatedly enter incorrect shared secret passwords no longer cause all of the resources for their VPN group to be used up by “ghost” connections. This condition only occurred when the concentrator used a server certificate and RADIUS.

- CSCdu23028

  The concentrator no longer restarts due to an effect the fiberchannel fastsend function had on the packet buffer queue.

- CSCdu34705

  When a LAN-to-LAN tunnel is initiated by a VPN device using a CheckPoint firewall, the concentrator no longer restarts.

Caveats Fixed in Version 5.2.19

This section lists caveats fixed in software Version 5.2.19.

- CSCco00582

  When a user connects to a VPN 5002 or 5008 concentrator using RADIUS, statistics for the connection on slots other than slot 0 are now correctly logged in the log file.

- CSCco00620

  The **show sys hardware** command now correctly displays Ethernet speeds.

- CSCco00999

  In cases in which not all slots in a VPN 5002 or 5008 are filled, the **show version** command no longer prints an erroneous message on the console.

- CSCdr53664

  The **show vpn user** command no longer displays invalid information for VPN users with RADIUS authentication.

- CSCdr63464

  When you configure bridging in a LAN-to-LAN tunnel, the concentrator no longer makes the Bridge port a VPN-only port and now responds to all traffic.

- CSCds36058

  If a tunnel connecting to a dynamic responder (**Tunnel Partner VPN Default** section) disconnects and then reconnects, the routing table on the concentrator now updates to use the new tunnel.

- CSCds36488

  When client connections do not complete authentication, the resources are no longer held and the tally for sessions in negotiation does not continue to increase.

- CSCds39150

  The failure to define a value for the shared key in the **Tunnel Partner** section no longer causes a boot-loop condition when you use Main mode tunnel initiation.

- CSCds40191

  The **show ipx runtime** command no longer displays an incorrect value for the net number when the directly connected routing table is built correctly.

- CSCds40811

  The concentrator now sends the correct TTL in ICMP packets.

- CSCds67955

  Invalid parameters in the **reset tcp socket all** command no longer cause a device restart.

Caveats Fixed in Version 5.2.16

This section lists caveats fixed in software Version 5.2.16.

- CSCco00501

  When configuring IPX for a LAN-to-LAN tunnel, the **show ipx route** command no longer indicates that the bind to address is the ip vpnxx port. It now indicates the correct bound to port address.

- CSCco00749

  If you configure multiple VPN-only ports on a VPN 5008 concentrator, all traffic to or from a given VPN-only port is no longer sent only to Ethernet 0:0.

- CSCco00938

  KeepAlive packets now pass through a NAT device correctly.

- CSCco01065

  The accounting function now works correctly with the Livingston Version 2.1 RADIUS server.

- CSCco01108

  The VPN 5000 client for Windows 2000 can now Telnet through an established VPN tunnel to any other VPN 5000 concentrator connected on that same subnet.

- CSCdr60383

  The concentrator can now use a server certificate based on a key length greater than 2048 bits.

- CSCdr68358

  Using the **telnet** command *source_address* option no longer restarts the concentrator.

- CSCdr93679

  The RADIUS Acct-Session-Time no longer accrues successive attempts to send accounting stop packets from the VPN 5000 concentrator to the RADIUS server.

- CSCdr93842

  RADIUS accounting stop packets now contain the user name.

- CSCdr95812

  You can now close LAN-to-LAN tunnels on a dynamic responder (**Tunnel Partner VPN Default** section) using the **vpn tunnel down** command.

- CSCds01953

  IP packets that have the TOS field set (the same as in VoIP and QoS applications) now have that information copied into the IPSec packet header when it gets tunneled.

- CSCds02352

  If a RADIUS server is defined but unreachable, the **Radius** section **SecAddress** keyword is set to 0.0.0.0, and a certificate is present in the concentrator, a restart event no longer occurs.

- CSCds03578

  Assigning IP addresses to clients from a RADIUS server now works.

- CSCds13425

  SecurID processing no longer fails and no longer presents the following log message:

  ```
  Notice   8/24/00 4:48:30 -- reason: S_SECURID_FAILURE (254@2311)
  ```

- CSCds14573

  If a VPN group's connect timeout is reached, VPN clients in a group with the **VPNGroupDLCI** keyword no longer become disconnected from a DS3 card on a VPN 5002 concentrator.

- CSCds21213

  When you use the VPN 5000 Manager to issue the **reset tcp socket all** command, the concentrator no longer reboots.

- CSCds31492

  RADIUS stop packets are now sent correctly.

Caveats Fixed in Version 5.2.15

This section lists caveats fixed in software Version 5.2.15.

- CSCdr44717

  If the main server stops responding, the **BackupServer** keyword in the **SecurID** section now works to allow the concentrator to use a backup SecurID server.

- CSCdr53740

  If you use SecurID with the **VPN Users** section, but also use RADIUS for accounting, the concentrator now returns the SecurID user name to the RADIUS server, not just the **VPN Users** name, which might be a shared login for multiple users.

- CSCdr59880

  When you use the **show vpn users** and **show vpn partners** commands, the concentrator now displays the VPN port number instead of the internal interface. Only the VPN port number (not the internal interface number) can be used to reset VPN connections using the **reset vpn** command.

- CSCdr60803

  The **boot** command now works over Telnet.

- CSCdr78162

  The VPN 5000 concentrator now returns attribute 25 to a RADIUS server when addresses are assigned from a RADIUS IP address pool.

Caveats Fixed in Version 5.2.14

This section lists caveats fixed in software Version 5.2.14 from Compatible Systems IntraPort Version 5.1.x. IntraPort servers are now called the Cisco VPN 5000 concentrator series.

- CSCco00281

  G2 now works for the **IKE Policy** section. The **IKE Policy** section keyword and argument **protection =** *xxx*_*yyy*_**G2** now works, where *xxx* = MD5 or SHA, and *yyy* = DES or 3DES.

- CSCco00425

  If you press Ctrl-C during the display of a **show** command, this action no longer causes the concentrator to restart.

- CSCco00597

  LAN-to-LAN tunnels running IPX between two VPN 5001 concentrators no longer drop the connection after 15 minutes in rare conditions.

- CSCco00712

  IP packet filters on the VPN 5002 or 5008 concentrator now work correctly on cards installed in slots other than slot 0.

- CSCco00764

  When the VPN 5000 client for Windows NT connects to slot 1, a traceroute from a DOS shell no longer displays the first hop as 76.0.0.1.

- CSCco00814

  A tunnel between an IntraPort 2+ and an IntraPort 2 no longer suddenly stops routing traffic. Formerly, when an IntraPort 2+ used both Ethernet connections and the IntraPort 2 used only one connection, if a packet generated by the IntraPort 2+ was sent directly to the Intraport 2 over the tunnel, the tunnel stopped routing across the tunnel.

- CSCco00962

  The IntraPort 2+ no longer reboots under rare conditions with heavy traffic.

- CSCco00976

  The **SecurIDRequired = On** keyword in the **VPN Group** section no longer overrules the **Enabled = Off** keyword in the **SecurID** section. Formerly, the **SecurID** section keyword was ignored.

- CSCco00997

  When a client connects from the LAN connected directly to the concentrator, the ARP table no longer becomes corrupt.

- CSCco01041

  The VPN 5002 concentrator no longer occasionally restarts unexpectedly during its normal boot process.

- CSCco01072

  Macintosh VPN users using SecurID are now deleted after terminating the tunnel. Formerly, the concentrator stopped accepting connections because unconnected users still used up system resources. The output from the **show vpn users** command showed no users connected, but the **show os vpn** command showed connections. The maximum number of connections had been exceeded.

- CSCco01130

  CiscoSecureNT no longer fails for user authentication. Formerly, the CiscoSecureNT server tagged the Tunnel-Password values when the server returned the values to the concentrator.

- CSCco01147

  OSPF route aggregation no longer causes a VPN 5001 concentrator to restart.

- CSCco01160

  Heavy traffic, such as heavy XWindows use, no longer causes a VPN 5001 concentrator to restart.

- CSCco01193

  Switch 9 on the test switch in slot 0 no longer causes lack of connectivity to other slots.

- CSCdr33183

  SecurID passcodes greater than 16 characters no longer disable further authentication. Formerly, if your VPN group specified the VPN username to be used as the SecurID username (**SecurIDUsername = False**), and your passcode was more than 16 characters, you could not connect after that attempt even with the proper passcodes. No other users in a VPN group with **SecurIDUsername = False** could connect either.

- CSCdr42036

  The **show os state** command no longer displays the enabled password without being enabled.

- CSCdr43915

  The Ethernet port no longer begins processing packets before other stacks are initialized. Formerly, this action caused the concentrator to restart at boot time while other processes completed initialization.

Closed Caveats

The following sections list known issues with the VPN 5000 concentrator software Version 5.2.22. A closed caveat is one that Cisco does not intend to fix. They are included here for reference and for the valuable workarounds (when available).

General System Caveats

- CSCdr63646

  When you use IPX packet filters on the VPN 5002 or 5008 concentrator, cards installed in slots other than slot 0 might not filter all packets correctly.

  No workaround.

- CSCdr71541

  The **certificate remove** command does not work, so you cannot remove a root or server certificate from the concentrator.

Workaround: If you want to prevent connectivity to the concentrator, revoke the certificate on the CA. If you created the certificate from a CG, create a new root certificate and install it on the concentrator so that the server certificate does not match.

- CSCds17529

  When you use the VPN 5000 MIB for the VPN 5001 concentrator, several variables return values of zero. The variables are:

  – CPU utilization

  – Tunnel Latency

  – Tunnel Bandwidth Out

  – Tunnel Bandwidth Return

  Workaround: Set the **Tunnel Partner** section **SlaEnablePartner** keyword to **On** for the tunnels in question.

- CSCds87290

  When you use the **show sys hardware** command on a VPN 5002 or VPN 5008 concentrator, only statistics for the card in slot 0 appear.

  No workaround.

- CSCdu02985

  The concentrator randomly restarts when it attempts to decode an invalid packet due to a collision.

  No workaround.

- CSCdu71391

  VPN 5001 concentrators reboot spontaneously without saving a restart trace in software releases prior to 5.2.22 and 6.0.20. In software releases 5.2.22 and 6.0.20 and later, a restart event is saved, similar to the following example. If the EXCEPTION field has the word Reset next to it, and the Control Register under the StrongARM MMU Registers heading has a value ending with 70, then your device has a hardware problem.

  Workaround: Please contact the Cisco Technical Assistance Center to replace your unit.

```
Restart Information:
    System Uptime:    1 day 17 hours 33 minutes 47 secs
    Time:             9/21/01 9:06:35
    OS Version:       IntraPort2+ V5.2.21.0005 (dalecki) US
    Panic Code:       0x00006ff9
    Panic Info:       0x00000000 0x00000000 0x00000000

 EXCEPTION: Reset

 Registers:
      R0   0x003d9430   R1   0xffff66af
      R2   0x002bdb04   R3   0x0000ffff
      R4   0xf03d9444   R5   0x00000000
      R6   0x0004994c   R7   0x000065af
      R8   0x00000000   R9   0x0000007f
      R10  0x00000000   FP   0x00212a54
      R12  0x00000000   SP   0x003fec88
      LR   0x41000d98   PC   0x41000d98
      CPSR 0x600000d3 (13)

 StrongARM MMU Registers:
       ID Register            4401a103
       Control Register       00264070  <   ending with the value of "70" means that
the MMU was turned off and the processor reseted.
```

```
       TLB Register           00264070
       Domain Register        11111110
       Fault Status Register  00264054
       Fault Address Register 00000000
       Saved CPSR             000000d3

 Process Info:
      name -> 'prnull',  priority/state -> 6/0x3
      plimit/pbase/size  -> 0x00215c04/0x00216c00/4096

 Backtrace:
      fp 0x00212a54, rtn 0x00169e70, args: <not available>
      fp 0x00212a8c, rtn 0x00385158, args: <not available>
      fp 0x003851fe, rtn 0x88b8b0e2, args: <not available>

 Stack:  0x003fec54
 003fec54  0000 0005 2e7c 3762  ac88 242c 43ba 9e41  *.....|7b..$,C..A*
 003fec64  0def 07ac 6558 7a3f  f03d 9444 0000 0000  *....eXz?.=.D....*
```

- CSCdv75940

  If you set the **IP** section **OSPFEnabled** keyword to **Passive** on Ethernet 0:0, OSPF fails to initialize at startup.

  Workaround: Set **OSPFEnabled** to **On** for Ethernet 0:0, and use route filters (**IP Route Filter** section) to keep the routes from going out the interface. Or upgrade to Version 6.0.x for full OSPF functionality.

- CSCdw19706

  You cannot use a WAN port IP address as the source address in the ping command.

  Workaround: Upgrade to Version 6.0.x.

- CSCdw19736

  If you configure multiple subinterfaces, the **show ip config** command displays duplicate entries for the interfaces.

  No workaround.

- CSCdw20272

  Frame Relay connections are unstable. Although the connection appears to be up when using the **show wan** command, the system log indicates the connection is up intermittently. The VPN 5000 concentrator cannot successfully ping remote devices, and remote pings succeed only occasionally. This caveat occurs in Version 5.2.19 and later.

  Workaround: Upgrade to Version 6.0.x.

- CSCdw39372

  If the SNMP administrator issues a get on the SNMPv2 MIB II UDP group, no information is returned for the UDP table.

  No workaround.

ESP Card and Port Caveats

- CSCco00572

  When you unplug the Ethernet port from the network and then reconnect it, it does not renegotiate its speed or duplex setting correctly in auto detect mode.

Workaround: Connect the Ethernet cable to the hub or switch, and turn off the concentrator and then turn it on.

VPN Tunneling Caveats

- CSCco00618

  Netware Directory Services does not work correctly over a VPN tunnel; the Neat16.exe and Nal.exe applications do not run.

  Workaround: NWAdmin.exe runs correctly and can be used instead.

- CSCco00741

  Under rare conditions, numbered VPN tunnels that are opening and closing can fill an IP broadcast table, preventing further tunnels from opening. Check the system log for "IP Broadcast hash full" errors.

  Workaround: Restart the concentrator.

- CSCco00914

  If you configure a **WINSPrimaryServer** or **WINSSecondaryServer** in the **VPN Group** section, this configuration does not forward WINS traffic from the client correctly. Normally, specifying a WINS server on the concentrator redirects any client WINS traffic over the tunnel, regardless of the WINS server configured on the client PC. However, while the client can see hosts in the Network Neighborhood, the client receives an error message when it attempts to connect.

  Workaround: Instruct the client user to configure the remote WINS servers in the Network Control Panel or in the dial-up profile, and not to specify a WINS server on the concentrator.

- CSCdr28216

  The Solaris VPN 5000 client does not tunnel any traffic without an **IPNet** defined in the **VPN Group** section. It should tunnel all traffic.

  Workaround: Configure the **VPN Group** with an **IPNet** value.

- CSCdt74495

  You are not able to establish a LAN-to-LAN tunnel between two VPN 5000 concentrators when one is set up as initiator, and the other as responder. This condition may occur with the following configurations:

  – Configuration 1— The tunnel is configured for Aggressive mode, and the Main mode keywords **LocalAccess** or **Peer** are defined. These keywords are only used for Main mode tunnels.

    Workaround: Delete the **LocalAccess** and **Peer** keywords from the configuration.

  – Configuration 2— The tunnel is configured for Main mode, and the **LocalAccess** and **Peer** keywords establish routes that duplicate routes that are configured in the **IP Static** section.

    Workaround: Remove the duplicate static route from the **IP Static** section.

- CSCdv89759

  If you are using OSPF, and you configure a standard IPSec tunnel using the **Tunnel Partner** section **LocalAccess** and **Peer** keywords, a static route is installed for the tunnel. If you take the tunnel down using the **vpn tunnel down** command, the concentrator never informs neighboring routers that the static route was removed, so the route continues to exist in neighbor routing tables.

  Workaround: We suggest you upgrade to Version 6.0.x for full OSPF functionality.

- CSCdw18710

  If you enable OSPF on a GRE tunnel between the concentrator and a Cisco IOS device, and you enter **show ip route** or ping the other end of the tunnel, the concentrator might restart.

  Workaround: We suggest you upgrade to Version 6.0.x for full OSPF functionality.

User Authentication Caveats

- CSCco01036

  The **show os netif** command displays extra or duplicate netif entries for a VPN 5000 concentrator with only Ethernet 0 connected. The command shows entries for the unconnected slot 1:

```
66 nivpn1:0    66   0   0  -               Down          0
66 nivpn1:0    66   0   0  -               Up            0
```

  No workaround.

- CSCdr33248

  The **reset vpn all** command or the legacy **reset step all** command does not clear all client and LAN-to-LAN tunnels. Normally, these commands clear all active tunnels from the device. Sometimes, however, some “ghost” tunnel connections may be persistent. Ghosts do not have an active client or LAN-to-LAN tunnel, but statistics claim that there are connections to these ghosts. Ghosts do not claim system resources or use processing time, but can claim IP addresses and connections within a VPN group and reduce the maximum number of connections for the device. A small number of ghosts are considered harmless and are usually created by rare connection attempts that go awry.

  Workaround: Enter the **reset vpn all** command two times to clear all client and LAN-to-LAN tunnels, including ghosts. To expel persistent ghosts, reboot the concentrator.

- CSCds27007

  You cannot assign a SecurID username with an at symbol (@); the SecurID server does not allow the at symbol in a username.

  Workaround: Do not use at symbols in user names, or upgrade to Version 6.0, which converts the at symbol to a question mark (?).

- CSCds34591

  If multiple clients attempt to connect to the VPN 5000 concentrator using SecurID, and the concentrator has not yet established the password between itself and the ACE/Server (usually established on the first connection), then the ACE/Server reports, “ACCESS DENIED, Can’t lock client,” and fails to authenticate the clients.

  Workaround: Use only one client to connect to the concentrator for the first SecurID authentication, allowing the concentrator to establish the password correctly. After the password is set, clients can connect normally, including to create simultaneous connections.

- CSCds56570

  The default value for the **Radius** section **VPNGroupInfo** keyword is 77. This setting is in violation of RFC 2869, which states that attribute 77 should be used for data *from* the concentrator *to* the RADIUS server, and not the other way around.

  Workaround: Set this value to another number, such as 88.

- CSCdu31499

  The **show radius config** command shows the secondary RADIUS server as “Off” even if it is configured. This display does not affect functionality.

  No workaround.

- CSCdu31506

  The **Radius** section **SecAddress** keyword does not work properly when set to a domain name.

  Workaround: Set an IP address.

- CSCdv22824

  When an internal concentrator interface fails (for example, losing the connection to a RADIUS server), client failover to a secondary concentrator could take as long as 70 seconds.

  No workaround.

IPX Caveats

- CSCdu44536

  When you enter the **show ipx runtime** command, the concentrator only shows the dynamically connected IPX net numbers if the client is terminated on slot 0.

  No workaround.

AppleTalk and VPN Caveats

- CSCco01007

  The **show appletalk config** command for a VPN interface displays limited or no AppleTalk information.

  For example, if you configure AppleTalk as follows:

```
[ AppleTalk VPN 0 ]
Mode                    = Routed
Seed                    = Seed
NetLower                = 3101
Node                    = 1
DefZone                 = "Fibre WAN-x"
Updates                 = Periodic
```

  The **show** commands appear as:

```
#show appletalk config
Port       Phase   Seed  Netnum         Node  Zone Name
Ether0         1   ** Disabled **
Ether0         2   ** Disabled **
Ether1         1   ** Disabled **
Ether1         2   ** Disabled **
Bridge         1   ** Disabled **
Bridge         2   ** Disabled **
VPN0                                  1

NBP Filters:
                     Stay in    Lookups    Tilde     Laser-
Port       Phase   zone?      In  Out    Devices   Writers
Ether0         1   ** Disabled **
Ether0         2   ** Disabled **
Ether1         1   ** Disabled **
```

```
Ether1          2    ** Disabled **
Bridge          1    ** Disabled **
Bridge          2    ** Disabled **

Appletalk Zone List:
```

Workaround: Try to issue the command several times and verify interface settings using **show appletalk config vpn** *number.*

- CSCdt40761

  If you use the command line interface to configure AppleTalk parameters for an Ethernet interface, the concentrator sends an invalid section name error message.

  No workaround.

- CSCdv89777

  For AppleTalk routing to work across an IPSec LAN-to-LAN tunnel, the **AppleTalk** section keyword **NetLower** keyword must be set to a legal value.

  Workaround: Set the **NetLower** keyword.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through 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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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:

Cisco Systems
Attn: Document Resource Connection
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 by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.