Cisco Easy VPN Remote Feature

OL-1748-02 Rev B0
November 20, 2002

Feature History

Release	Modification
12.2(4)YA	This feature was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support for this feature was added to the Cisco IOS Release 12.2 T train for the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers. (Cisco IOS Release 12.2(13)T does not support this feature on any Cisco 800 series routers.)

This document describes the Cisco Easy VPN Remote feature for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers. This document provides information on configuring and monitoring the Cisco Easy VPN Remote feature to create IPSec Virtual Private Network (VPN) tunnels between a supported router and another Cisco router that supports this form of IPSec encryption/decryption.

Note At the time of this document's publication, the Cisco Easy VPN Remote Phase II feature has been released in Cisco IOS Release 12.2(8)YJ and Cisco IOS Release 12.2(15)T. Cisco recommends using the Phase II feature on Cisco IOS Release 12.2(15)T, as documented in the *Cisco Easy VPN Remote Phase II Feature* document. If you want to use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended.

This document includes the following major sections:

Feature Overview

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated, and typically requires tedious coordination between network administrators to configure the two routers' VPN parameters.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco's Unity Client protocol, which allows most VPN parameters to be defined at a VPN remote access server. This server can be a dedicated VPN device such as a VPN 3000 concentrator or a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.

After the VPN remote access server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a Cisco uBR905 or Cisco uBR925 cable access router, as well as on the Cisco 806/826/827/828 and Cisco 1700 series routers. When the IPSec client then initiates the VPN tunnel connection, the VPN remote access server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Automatically creating the NAT/PAT translation and associated access lists that are needed, if any.
- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

The Cisco Easy VPN Remote feature supports two modes of operation:

- Client—Specifies that Network Address Translation/Port Address Translation (NAT/PAT) be done, so that the PCs and other hosts at the client end of the VPN tunnel form a private network that does not use any IP addresses in the destination server's IP address space.

  In client mode, the Cisco Easy VPN Remote feature automatically configures the NAT/PAT translation and access lists that are needed to implement the VPN tunnel. These configurations are automatically created when the IPSec VPN connection is initiated. When the tunnel is torn down, the NAT/PAT and access list configurations are automatically deleted.

  The NAT/PAT configuration is created with the following assumptions:

  – The **ip nat inside** command is applied to the FastEthernet0 (Cisco 1700 series) or Ethernet0 (Cisco 806, Cisco 826, Cisco 827, Cisco 828 routers, Cisco uBR905, Cisco uBR925) interface.

  – The **ip nat outside** command is applied to the interface that is configured with the Cisco Easy VPN Remote configuration. (On the Cisco uBR905 and Cisco uBR925 routers, this is always the Cable-modem0 interface. On the Cisco 800 series and Cisco 1700 series routers, this will be the WAN interface configured with the Cisco Easy VPN Remote configuration.)

Tip The NAT/PAT translation and access-list configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup or running configuration files. These configurations, however, can be displayed using the **show ip nat statistics** and **show access-list** commands.

Note Because the Cisco Easy VPN Remote feature automatically creates a NAT/PAT configuration for the VPN tunnel, you must not create a manual NAT/PAT configuration on any interface when using the Cisco Easy VPN Remote feature. If NAT/PAT has already been configured on the router, you must remove that configuration before beginning the Cisco Easy VPN Remote configuration.

- Network Extension—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network, so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network.

Both modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an ISP or other service (thereby eliminating the corporate network from the path for Web access).

Authentication can also be done using Extended Authentication (XAUTH). In this situation, when the VPN remote access server requests XAUTH authentication, the following messages are displayed on the router's console:

```
EZVPN: Pending XAuth Request, Please enter the following command:
EZVPN: crypto ipsec client ezvpn xauth
```

The user can then provide the necessary user ID, password, and other information by entering the **crypto ipsec client ezvpn xauth** command and responding to the following prompts.

Note The timeout for entering the username and password is determined by the configuration of the VPN remote access server. For servers running Cisco IOS software, this timeout value is specified by the **crypto isakmp xauth timeout** command.

Figure 1 illustrates the client mode of operation. In this example, the Cisco uBR905 cable access router provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the Cisco uBR905 router, which also has an IP address in the 10.0.0.0 private network space. The Cisco uBR905 router performs NAT/PAT translation over the VPN tunnel, so that the PCs can access the destination network.

Figure 1 Cisco Easy VPN Client Connection

Note The diagram in Figure 1 could also represent a split tunneling connection, in which the client PCs can access public resources in the global Internet without including the corporate network in the path for the public resources.

Figure 2 on page 5 also illustrates the client mode of operation, where a VPN concentrator provides destination endpoints to multiple xDSL clients. In this example, Cisco 800 series routers provide access to multiple small business clients, each of which uses IP addresses in the 10.0.0.0 private network space. The Cisco 800 series routers perform NAT/PAT translation over the VPN tunnel, so that the PCs can access the destination network.

Figure 2 Cisco Easy VPN Client Connection (using VPN concentrator)

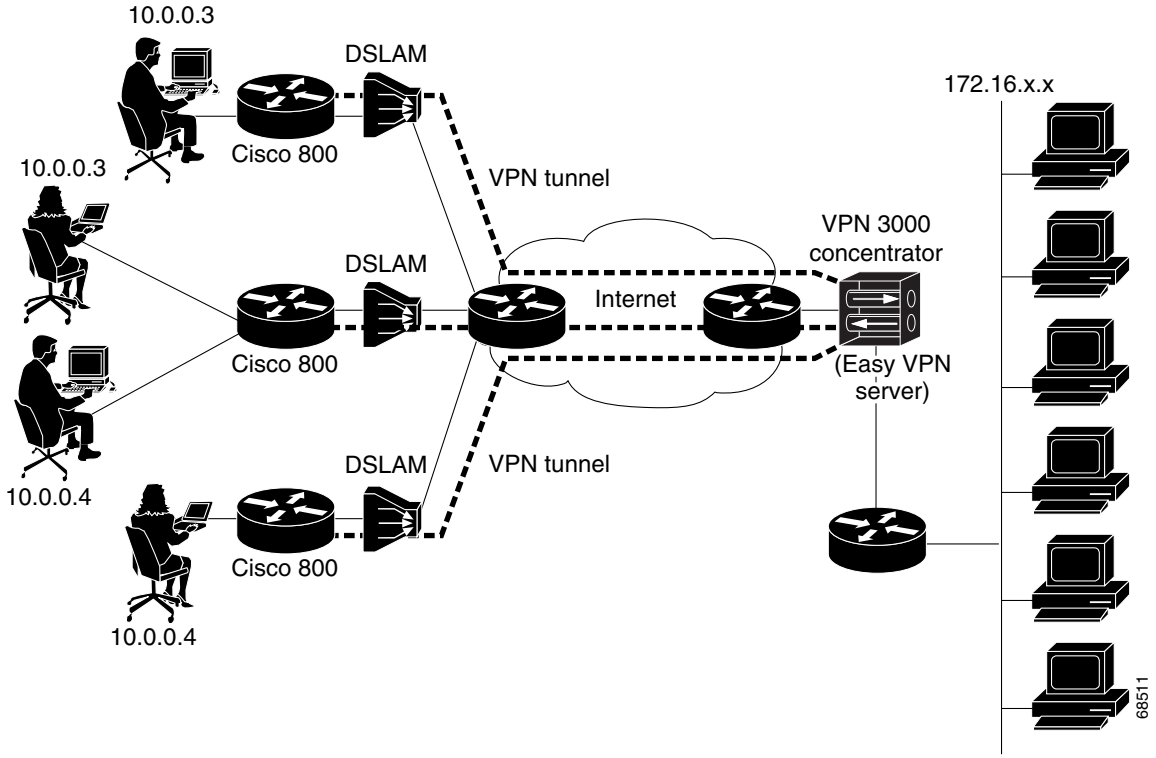

Figure 3 on page 6 illustrates the network extension mode of operation. In this example, the Cisco uBR905 cable access router and Cisco 1700 series router both act as Cisco Easy VPN Remotes, connecting to a VPN 3000 concentrator.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network, or they could also be in separate subnets, as long as the destination routers are configured to properly route those IP addresses over the tunnel.

In this example, the PCs and hosts attached to the two routers have IP addresses that are in the same address space as the destination enterprise network. The PCs connect to the Cisco uBR905 router's Ethernet interface, which also has an IP address in the enterprise address space. This provides a seamless extension of the remote network.

Figure 3 Cisco Easy VPN Network Extension Connection

Note For information on configuration the VPN 3000 concentrator for use with the Cisco Easy VPN Remote feature, please see the "Configuring the VPN 3000 Series Concentrator" section on page 18.

Benefits

- The centrally stored configurations allow dynamic configuration of end-user policy, required less manual configuration by end-users and field technicians, reducing errors and further service calls.
- The local VPN configuration is independent of the remote peer's IP address, allowing the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management.
- Enables large-scale deployments with rapid user provisioning.
- Removes the need for end-users to purchase and configure external VPN devices.
- Removes the need for end-users to install and configure VPN client software on their PCs.
- Offloads the creation and maintenance of the VPN connections from the PC to the router.
- Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.

Restrictions

No Manual NAT/PAT Configuration Allowed

The Cisco Easy VPN Remote feature automatically creates the appropriate NAT/PAT configuration for the VPN tunnel. You therefore must not create a manual NAT/PAT configuration on any interface when using the Cisco Easy VPN Remote feature. If NAT/PAT has already been configured on the router, you must remove that configuration before beginning the Cisco Easy VPN Remote configuration.

Only One Destination Peer Supported

The Cisco Easy VPN Remote feature supports the configuration of only one destination peer and tunnel connection. If your application requires the creation of multiple VPN tunnels, you must manually configure the IPSec VPN and NAT/PAT parameters on both the client and server.

Change of IP Address on Inside Interface

Changing the IP address on the inside interface automatically resets the Cisco Easy VPN Remote connection so that the new IP address can be implemented on the tunnel connection.

Required Destination Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a VPN remote access server or VPN concentrator that supports either the VPN Remote Access Server Enhancements feature or the Cisco Unity protocol. At the time of publication, this includes the following platforms when running the indicated software releases:

- Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers—Cisco IOS Release 12.2(4)YA or later
- Cisco 1700 series—Cisco IOS Release 12.2(4)YA or later
- Cisco 2600 series—Cisco IOS Release 12.2(8)T or later
- Cisco 3620—Cisco IOS Release 12.2(8)T or later
- Cisco 3640—Cisco IOS Release 12.2(8)T or later
- Cisco 3660—Cisco IOS Release 12.2(8)T or later
- Cisco 7100 series VPN routers—Cisco IOS Release 12.2(8)T or later
- Cisco 7200 series routers—Cisco IOS Release 12.2(8)T or later
- Cisco 7500 series routers—Cisco IOS Release 12.2(8)T or later
- Cisco uBR905 and Cisco uBR925 cable access routers—Cisco IOS Release 12.2(4)YA or later
- Cisco VPN 3000 series—Software Release 3.11 or later
- Cisco PIX 500 series—Software Release 6.0 or later

Note Unless otherwise indicated, the above platforms must be running either Cisco IOS Release 12.2(13)T, Cisco IOS Release 12.2(8)T, or later, to provide Cisco Unity server support.

Digital Certificates Not Supported

In Cisco IOS Release 12.2(13)T, the Cisco Easy VPN Remote feature does not support authentication using digital certificates. Authentication is supported using preshared keys and Extended Authentication (XAUTH).

Only ISAKMP Policy Group 2 Supported on IPSec Servers

The Unity Protocol supports only ISAKMP policies that use group 2 (1024-bit Diffie-Hellman) IKE negotiation, so the IPSec server being used with the Cisco Easy VPN Remote must be configured for a group 2 isakmp policy. The IPSec server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN Remote.

Perfect Forward Secrecy Not Supported

The Cisco Easy VPN Remote feature does not support the Perfect Forward Secrecy (PFS) feature that is available on the Cisco VPN 3000 concentrator.

Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (ESP-DES and ESP-3DES) or transform sets that provide authentication without encryption (ESP-NULL ESP-SHA-HMAC and ESP-NULL ESP-MD5-HMAC).

Changing the IP Address on the LAN Interface on Cisco 800 Series Routers

The Ethernet 0 LAN interface on the Cisco 800 series routers default to a primary IP address in the private network of 10.10.10.0. If you need to change this IP address to match the local network's configuration, you can use either the **ip address** CLI command or by using the Cisco Router Web Setup (CRWS) web interface.

However, these two techniques differ slightly in how the new IP address is assigned. When using the CLI command, the new IP address is assigned as the primary address for the interface. When using the CRWS interface, the new IP address is assigned as the secondary address, and the existing IP address is preserved as the primary address for the interface. This allows the CRWS interface to maintain the existing connection between the PC web browser and the Cisco 800 series router.

Because of this behavior, the Cisco Easy VPN Remote feature assumes that if a secondary IP address exists on the Ethernet 0 interface, the secondary address should be used as the IP address for the inside interface for the NAT/PAT configuration. If no secondary address exists, the primary IP address will be used for the inside interface address, as is normally done on other platforms. If this behavior is not desired, use the **ip address** CLI command to change the interface's address, instead of using the CRWS web interface.

USB Interface Not Supported on the Cisco uBR925 Router

The Cisco Easy VPN Remote feature supports only the Ethernet interface on the Cisco uBR925 cable access router. The feature does not support the router's USB interface.

VPN 3000 Configuration

The configuration of the VPN 3000 concentrator has several restrictions when used with the Cisco Easy VPN Remote feature. See the "Configuring the VPN 3000 Series Concentrator" section on page 18 for more details.

Related Documents

This section lists other documentation related to the configuration and maintenance of the supported routers and the Cisco Easy VPN Remote feature.

Platform-Specific Documentation

Cisco 800 Series Routers

- *Cisco 806 Router Hardware Installation Guide*
- *Cisco 826 Router Hardware Installation Guide*
- *Cisco 827 Router Hardware Installation Guide*
- *Cisco 828 and SOHO 78 Routers Hardware Installation Guide*
- *Cisco 806 Software Configuration Guide*
- *Cisco 827 Router Software Configuration Guide*
- *Cisco 828 Router and SOHO 78 Router Software Configuration Guide*

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

Cisco uBR905 and Cisco uBR925 Cable Access Routers

- *Cisco uBR925 Cable Access Router Hardware Installation Guide*
- *Cisco uBR905 Hardware Installation Guide*
- *Cisco uBR905/uBR925 Cable Access Router Software Configuration Guide*
- *Cisco uBR925 Cable Access Router Subscriber Setup Quick Start* Card
- *Cisco uBR905 Cable Access Router Subscriber Setup Quick Start* Card
- *Cisco uBR925 Cable Access Router Quick Start User Guide*

Cisco 1700 Series Routers

- *Cisco 1700 Series Router Software Configuration Guide*
- *Cisco 1710 Security Router Hardware Installation Guide*
- *Cisco 1710 Security Router Software Configuration Guide*
- *Cisco 1720 Series Router Hardware Installation Guide*
- *Cisco 1721 Access Router Hardware Installation Guide*
- *Cisco 1750 Series Router Hardware Installation Guide*
- *Cisco 1751 Router Hardware Installation Guide*
- *Cisco 1751 Router Software Configuration Guide*
- *Cisco 1760 Modular Access Router Hardware Installation Guide*

Also see the Cisco IOS release notes for Cisco IOS Release 12.2(4)YA:

- *SOHO 70 and Cisco 800 Series—Release Notes for Release 12.2(4)YA*

- *Release Notes for Cisco uBR905 and Cisco uBR925 Cable Access Routers for Cisco IOS Release 12.2 YA*
- *Cisco 1700 Series—Release Notes for Release 12.2(4)YA*

IPsec and VPN Documentation

For information on the VPN Remote Access Enhancements feature, which provides Cisco Unity client support for the Cisco Easy VPN Remote feature, see the *VPN Remote Access Enhancements* feature module for Cisco IOS Release 12.2(8)T.

For general information on IPSec and VPN subjects, see the following information in the product literature and IP technical tips sections on Cisco.com:

- *Deploying IPsec*—Provides an overview of IPsec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics.
- *Certificate Authority Support for IPsec Overview*—Describes the concept of digital certificates and how they are used to authenticate IPsec users.
- *An Introduction to IP Security (IPsec) Encryption*—Provides a step-by-step description of how to configure IPsec encryption.

The following technical documents, available on Cisco.com and the Documentation CD-ROM, also provide more in-depth configuration information:

- *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.2—Provides an overview of Cisco IOS security features.
- *Cisco IOS Security Command Reference*, Cisco IOS Release 12.2—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features.
- *Cisco IOS Software Command Summary*, Cisco IOS Release 12.2—Summarizes the Cisco IOS commands used to configure all Release 12.1 security features.

Note Additional documentation on IPsec becomes available on Cisco.com and the Documentation CD-ROM as new features and platforms are added. Cisco Press also publishes several books on this subject—go to http://www.ciscopress.com for more information.

Supported Platforms

The Cisco Easy VPN Remote client feature described in this document supports the following platforms:

- Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers
- Cisco uBR905 and Cisco uBR925 cable access routers
- Cisco 1700 series routers

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

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

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

The following new or modified MIBs are supported by this feature:

- CISCO-IPSEC-FLOW-MONITOR-MIB—Contains attributes describing IPSec-based VPNs (IETF IPSec Working Group Draft).
- CISCO-IPSEC-MIB—Describes Cisco implementation-specific attributes for Cisco routers implementing IPSec VPNs.
- CISCO-IPSEC-POLICY-MAP-MIB—Extends the CISCO-IPSEC-FLOW-MONITOR-MIB to map dynamically instantiated structures to the policies, transforms, cryptomaps, and other structures that created or are using them.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The following requirements are necessary to use the Cisco Easy VPN Remote feature:

- A Cisco 806, Cisco 826, Cisco 827, and Cisco 828 router, Cisco 1700 series router, or Cisco uBR905 or Cisco uBR925 cable access router running Cisco IOS Release 12.2(13)T or later, configured as an Cisco Easy VPN Remote.

- Another Cisco router or VPN concentrator that supports the VPN Remote Access Server feature or the Unity Client protocol and configured as a VPN remote access server. See the "Required Destination Servers" section on page 7 for a detailed list.

Configuration Tasks

See the following sections for configuration tasks for the Cisco Easy VPN Remote feature. Each task in the list is identified as either required or optional.

Configuring the DHCP Server Pool (Required for Client Mode)

The local router uses the DHCP protocol to assign IP addresses to the PCs that are connected to the router's LAN interface. This requires creating a pool of IP addresses for the router's onboard DHCP server. The DHCP server then assigns an IP address from this pool to each PC when it connects to the router.

In a typical VPN connection, the PCs connected to the router's LAN interface are assigned an IP address in a private address space. The router then uses NAT/PAT to translate those IP addresses into a single IP address that is transmitted across the VPN tunnel connection.

Tip Configuring the DHCP server pool is not normally needed on the Cisco 800 series routers because this is automatically done when using the Cisco Router Web Setup (CRWS) web interface that is available on those routers. Also, the DHCP server pool is not normally needed if using a router, such as the Cisco 827, with an ATM interface configured for PPPoE connections.

Use the following procedure to configure the DHCP server pool on the Cisco uBR905/uBR925 cable access routers and the Cisco 1700 series routers:

	Command	Purpose
Step 1	`Router(config)# ip dhcp pool pool-name`	Creates a DHCP Server address pool named *pool-name* and enters DHCP pool configuration mode.
Step 2	`Router(dhcp-config)# network ip-address [mask | /prefix-length]`	Specifies the IP network number and subnet mask of the DHCP address pool that is to be used for the PCs connected to the router's local Ethernet interface. This network number and subnet mask must specify the same subnet as the IP address assigned to the Ethernet interface. The subnet mask can also be specified as a prefix length that specifies the number of bits in the address portion of the subnet address. The prefix length must be preceded by a forward slash (/).

	Command	Purpose
Step 3	`Router(dhcp-config)# default-router` *address* `[`*address2 ... address8*`]`	Specifies the IP address of the default router for a DHCP client. You must specify at least one address. You can optionally specify additional addresses, up to a total of eight addresses per command. **Tip** The first IP address for the **default-router** option should be the IP address that is assigned to the router's Ethernet address.
Step 4	`Router(dhcp-config)# import all`	Imports the following DHCP option parameters from a central DHCP server into the router's local DHCP database: • Domain Name • DNS Server • NetBIOS WINS Server **Note** This option requires that a central DHCP server be configured to provide the DHCP options. The central DHCP server should be on the same subnet as was configured using the **network** option. (On Cisco IOS routers, this is done using the **ip dhcp database** command.) If you are using the PPP/IPCP protocol on the WAN interface, or the client on the WAN interface supports the Easy IP feature, the central DHCP server can be on a different subnet or network.
	Note You can also specify the DHCP option parameters manually by using the **domain-name**, **dns-server**, and **netbios-name-server** options but this is not recommended. Almost all installations should use the **import all** option to ensure that the router is configured with the proper DHCP parameters.	
Step 5	`Router(dhcp-config)# lease {`*days* `[`*hours*`][`*minutes*`] | infinite}`	(Optional) Specifies the duration of the DHCP lease. The default is a one-day lease.
Step 6	`Router(dhcp-config)# exit`	Leaves DHCP pool configuration mode.
Step 7	`Router(config)# ip dhcp excluded-address` *lan-ip-address*	Excludes the specified IP address from the DHCP server pool. The *lan-ip-address* should be the IP address assigned to the router's LAN interface (for example, the Ethernet0 on the Cisco uBR905/uBR925 routers and FastEthernet0 on the Cisco 1700 series routers).

Note The **ip dhcp pool** command supports a number of options for configuring the DHCP server pool. These other options are typically not needed for a Cisco Easy VPN Remote configuration.

Verifying the DHCP Server Pool

To verify that the DHCP server pool has been correctly configured, use the following procedure.

Step 1 Use the **show ip dhcp pool** command in Privileged EXEC mode to display the server pools that have been created:

```
Router# show ip dhcp pool
```

```
Pool localpool :
 Current index        : 192.168.100.1
 Address range        : 192.168.100.1 - 192.168.100.254
Router#
```

Step 2 If you used the **import all** option when you created the DHCP server pool, use the **show ip dhcp import** command to display the options that have been imported from the central DHCP server:

```
Router# show ip dhcp import

Address Pool Name: localpool
Domain Name Server(s): 192.168.20.5
NetBIOS Name Server(s): 192.168.20.6
Domain Name Option: cisco.com
Router#
```

Step 3 To display the IP addresses that the DHCP server has assigned, use the **show ip dhcp binding** command:

```
Router# show ip dhcp binding

IP address    Hardware address    Lease expiration        Type
192.168.100.3 00c0.abcd.32de      Nov 01 2001 12:00 AM    Automatic
192.168.100.5 00c0.abcd.331a      Nov 01 2001 12:00 AM    Automatic
Router#
```

Troubleshooting Tips

If PCs connected to the router's LAN interface cannot obtain an IP address using DHCP, check the following:

- Verify that the DHCP server has not been disabled on the router. The DHCP server is enabled by default, but it might have been disabled using the **no service dhcp** command. To check this, use the **show running-config** command:

  ```
  Router# show running-config | include dhcp
  no service dhcp
  ip dhcp pool localpool
  Router#
  ```

  If the output from the **show running-config** command does not include the **no service dhcp** command, the DHCP server is enabled.

- Use the **show ip dhcp binding** command to display the IP addresses that have already been assigned. Verify that the address pool has not been exhausted. If necessary, recreate the pool to create a larger pool of addresses.

- On a Windows PC that is connected to the router's LAN interface, use the **ipconfig /all** command to display its IP address configuration, including the DHCP server address.

  ```
  C:\> ipconfig /all

  Windows 2000 IP Configuration

         Host Name . . . . . . . . . . . . : MYPC-W2K1
         Primary DNS Suffix  . . . . . . . : cisco.com
         Node Type . . . . . . . . . . . . : Hybrid
         IP Routing Enabled. . . . . . . . : No
         WINS Proxy Enabled. . . . . . . . : No
         DNS Suffix Search List. . . . . . : cisco.com
  ```

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cisco.com
        Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : 01-23-45-67-89-AB
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.100.94
        Subnet Mask . . . . . . . . . . . : 255.255.254.0
        Default Gateway . . . . . . . . . : 192.168.100.1
        DHCP Server . . . . . . . . . . . : 172.16.156.54
        DNS Servers . . . . . . . . . . . : 172.16.168.183
                                            172.16.226.120
        Primary WINS Server . . . . . . . : 172.16.235.228
        Secondary WINS Server . . . . . . : 172.16.2.87
        Lease Obtained. . . . . . . . . . : Monday, October 22, 2001 11:15:32 A
        Lease Expires . . . . . . . . . . : Thursday, October 25, 2001 11:15:32 AM
```

Configuring and Assigning the Cisco Easy VPN Remote Configuration

The router acting as the IPSec client must create an Cisco Easy VPN Remote configuration and assign it to the outgoing interface. To do so, use the following procedure.

Note If you have previously configured NAT/PAT translation on the router, you must first remove that configuration before beginning the Cisco Easy VPN Remote configuration. Use the **show running-config | include nat** command to display any NAT/PAT configuration commands that might exist—if any commands appear, use the **no** form of the commands to remove that configuration before proceeding.

	Command	Purpose
Step 1	`router(config)# crypto ipsec client ezvpn` *name*	Creates an Cisco Easy VPN Remote configuration named *name* and enters Cisco Easy VPN Remote configuration mode.
Step 2	`router(config-crypto-ezvpn)# group` *group-name* **key** *group-key*	Specifies the IPSec group and IPSec key value to be associated with this configuration. **Note** The *group-name* must match the group defined on the IPSec server. On Cisco IOS routers, use the **crypto isakmp client configuration group** and **crypto map dynmap isakmp authorization list** commands. **Note** The *group-key* must match the key defined on the IPSec server. On Cisco IOS routers, use the **crypto isakmp client configuration group** command.
Step 3	`router(config-crypto-ezvpn)# peer` [*ip-address* | *hostname*]	Specifies the IP address or hostname for the destination peer. This is typically the IP address on the destination router's WAN interface. **Note** You must have a DNS server configured and available to use the *hostname* option.

	Command	Purpose
Step 4	`router(config-crypto-ezvpn)# mode {client | network-extension}`	Specifies the type of VPN connection that should be made: • **client**—Specifies that the router is configured for VPN client operation, using NAT/PAT address translation. • **network-extension**—Specifies that the router is to become a remote extension of the enterprise network at the destination of the VPN connection.
Step 5	`router(config-crypto-ezvpn)# exit`	Leaves Cisco Easy VPN Remote configuration mode.
Step 6	`router(config)# interface` *interface*	Enters interface configuration mode for the interface. This interface will become the "outside" interface for the NAT/PAT translation.
Step 7	`router(config-if)# crypto ipsec client ezvpn` *name*	Assigns the Cisco Easy VPN Remote configuration to the interface. This automatically creates the necessary NAT/PAT translation parameters and initiates the VPN connection. **Note** You can assign the Cisco Easy VPN Remote configuration to only one interface. You cannot assign the configuration to the interface that defaults to being the "inside" interface for the NAT/PAT translation. On the Cisco 1700 series routers this is the FastEthernet0 interface. On the Cisco 800 series routers this could be either the Ethernet0 or Dialer1 interface, depending on which is applicable. On the Cisco uBR905/uBR925 cable access routers, this is the Ethernet0 interface.
Step 8	`router(config-if)# exit`	Leaves interface configuration mode.
Step 9	`router(config)# exit`	Leaves global configuration mode.

Verifying the Cisco Easy VPN Configuration

To verify that the Cisco Easy VPN Remote configuration has been correctly configured, that the configuration has been assigned to an interface, and that the IPSec VPN tunnel has been established, use the following steps.

Step 1 Display the current state of the Cisco Easy VPN Remote connection using the **show crypto ipsec client ezvpn** command. The following is typical output for a router using client mode:

```
Router# show crypto ipsec client ezvpn
Current State: IPSEC ACTIVE
Last Event: SOCKET UP
Address: 198.1.1.90
Mask: 255.255.255.0
DNS Primary: 198.1.1.250
DNS Secondary: 198.1.1.251
NBMS/WINS Primary: 198.1.1.252
NBMS/WINS Secondary: 198.1.1.253
Router#
```

The following is typical output for a router using network-extension mode:

```
Router# show crypto ipsec client ezvpn
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
```

```
Address: 30.0.0.53
Mask: 255.255.255.255
Split Tunnel List: 1
       Address    : 30.100.0.0
       Mask       : 255.255.255.128
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Router#
```

Step 2 Display the NAT/PAT configuration that was automatically created for the VPN connection, using the **show ip nat statistics** command. The "Dynamic mappings" section of this display gives the details for the NAT/PAT translation that is occurring on the VPN tunnel.

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  cable-modem0
Inside interfaces:
  Ethernet0
Hits: 1489  Misses: 1
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 198 pool enterprise refcount 0
 pool enterprise: netmask 255.255.255.0
        start 198.1.1.90 end 198.1.1.90
        type generic, total addresses 1, allocated 0 (0%), misses 0\
Router#
```

Step 3 In client mode, the NAT/PAT translation one or more access lists that are also dynamically configured at the time the VPN tunnel is initiated. Display this access list using the **show access-list** command. The following is a typical display for a client configuration without split tunneling:

```
Router# show access-list
Extended IP access list 198
    permit ip 192.1.1.0 0.0.0.255 any
Router#
```

Note In this example, the Cisco Easy VPN Remote configuration creates access list 198 for the VPN tunnel NAT/PAT translation. The exact numbering of the access list can vary, depending on the other access lists that have been configured on the router. Do not assume that the VPN tunnel will use the same access list every time the connection is initiated.

The following is a typical display for a Cisco uBR905/uBR925 cable access router configured for client mode with split tunneling:

```
Router# show access-list
Extended IP access list 197
    deny ip 192.168.100.0 0.0.0.255 172.168.0.128 0.0.0.127
    deny ip 192.168.100.0 0.0.0.255 172.168.1.128 0.0.0.127
    permit ip 192.168.100.0 0.0.0.255 any
Extended IP access list 198
    permit ip 192.168.100.0 0.0.0.255 172.168.0.128 0.0.0.127
    permit ip 192.168.100.0 0.0.0.255 172.168.1.128 0.0.0.127
Router#
```

Tip Network extension mode without split tunneling does not need any access lists and thus does not create them. Network extension mode with split tunneling typically creates a single access list.

The following is a typical display for a Cisco 827 router configured for client mode with split tunneling:

```
c827# show access-list
Extended IP access list 197
    deny ip 70.0.0.0 0.255.255.255 30.100.0.0 0.0.0.127 (5 matches)
    permit ip 70.0.0.0 0.255.255.255 any
Extended IP access list 198
    permit ip 70.0.0.0 0.255.255.255 30.100.0.0 0.0.0.127 (5 matches)
c827#
```

Step 4 Display the destination IPSec peer and the key value being used with the **show crypto isakmp key** command:

```
Router# show crypto isakmp key
Hostname/Address       Preshared Key
193.1.1.1              hw-client-password
Router#
```

Configuring the VPN 3000 Series Concentrator

This section describes the guidelines required to configure the Cisco VPN 3000 series concentrator for use with Cisco Easy VPN Remotes. As a general rule, you can use the default configuration except for IP addresses, server addresses, and routing configurations, and for the following parameters and options:

Note You must be using software release 3.11 or later for the Cisco VPN 3000 series concentrator to support Cisco Easy VPN Remotes.

- IPSec Tunnel Protocol—Enable the IPSec tunnel protocol so it is available for users. This is configured on the VPN 3000 series concentrator by clicking the **General** tab on the **Configuration | User Management | Base Group** screen.
- IPSec group—Configure the VPN 3000 series concentrator with a group name and password that matches the values configured for the Cisco Easy VPN Remote configuration on the router. These values are configured on the router with the **group** *group-name* **key** *group-key* command, and are configured on the VPN 3000 series concentrator using the **Configuration | User Management | Groups** screen.
- Perfect Forward Secrecy—The Cisco Easy VPN Remote does not support the Perfect Forward Secrecy (PFS) option. This option must be set to **Disabled** in the **Configuration | Policy Management | Traffic Management | Security Associations** screens.
- Group Lock—If you are defining multiple users in multiple groups on the VPN 3000 series concentrator, you must check the **Group Lock** box in the IPSec tab to prevent users in one group from logging in with another group's parameters. For example, if you have configured one group for split tunneling access and another group without split tunneling access, the **Group Lock** will prevent users in the second group from gaining access to the split tunneling features. The Group Lock checkbox appears in the **IPSec** tab in the **Configuration | User Management | Base Group** screen and in the **IPSec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.
- XAUTH—To use extended authentication (XAUTH), set the **Authentication** parameter to **None**. The Authentication parameter appears in the **IPSec** tab in the **Configuration | User Management | Base Group** screen and in the **IPSec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

- Split Tunneling—The **Configuration | User Management | Base Group, Mode Configuration Parameters Tab** screen includes a **Split Tunnel** option with a checkbox that says "Allow the networks in the list to bypass the tunnel." When using the Cisco Easy VPN Remote feature, you must **not** click this checkbox because it is intended only for software VPN clients and will not work with hardware clients such as the Cisco Easy VPN Remote feature.
- IKE Proposals—The Cisco VPN 3000 Series Concentrator is preconfigured with a default IKE proposal, CiscoVPNClient-3DES-MD5, that can be used with Cisco Easy VPN Remotes. This IKE proposal supports preshared keys with extended authentication (XAUTH) using the MD5/HMAC-128 algorithm, and Diffie-Hellman Group 2.

  This proposal is active by default, but verify that it is still an active proposal using the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen.

  Note You can also use the default IKE proposals IKE-DES-MD5 and IKE-3DES-MD5, but they do not enable XAUTH support by default.

- Create a new IPSec Security Association—Cisco Easy VPN Remotes use a security association with the following parameters:
  - Authentication Algorithm=ESP/MD5/HMAC-128
  - Encryption Algorithm=DES-56 or 3DES-168 (recommended)
  - Encapsulation Mode=Tunnel
  - Digital Certificate=None (Use Preshared Keys)
  - IKE Proposal=CiscoVPNClient-3DES-MD5 (preferred)

  The Cisco VPN 3000 Series Concentrator is preconfigured with several default security associations but they do not meet the IKE Proposal requirements. To use an IKE Proposal of CiscoVPNClient-3DES-MD5, copy the ESP/IKE-3DES-MD5 security association and modify it to use CiscoVPNClient-3DES-MD5 as its IKE proposal. This is configured on the VPN 3000 series concentrator using the **Configuration | Policy Management | Traffic Management | Security Associations** screen.

Troubleshooting Tips

To troubleshoot a VPN connection created using the Cisco Easy VPN Remote, use the following suggested techniques.

- Enable debugging of the Cisco Easy VPN Remote feature using the **debug crypto ipsec client ezvpn** command.
- Enable debugging of IPSec and Internet Key Exchange (IKE) events using the **debug crypto ipsec** and **debug crypto isakmp** commands.
- Display the active IPSec VPN connections using the **show crypto engine connections active** command.
- To reset the VPN connection, use the **clear crypto ipsec client ezvpn** command. If you have debugging enabled, you might prefer to use the **clear crypto sa** and **clear crypto isakmp** commands.

Configuration Examples

This section provides the following configuration examples:

Client Mode Configurations

This section shows the following examples that demonstrate configurations for the Cisco Easy VPN Remote in the client mode of operation. Also shown are the VPN remote access server configurations that correspond to these client configurations.

Note Typically, users will configure the Cisco 800 series routers with the CRWS web interface, not by entering CLI commands. However, the configurations shown here for the Cisco 800 series routers display typical configurations that can be used if manual configuration is desired.

Cisco Easy VPN Client in Client Mode (Cisco uBR905/uBR925)

The following example configures a Cisco uBR905 cable access router as an IPSec client, using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- Routing mode—The **no cable-modem compliant bridge** command places the router in routing mode. IP routing, such as RIPv2, is not activated because the VPN configuration will direct all traffic to the destination point of the VPN tunnel.
- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the router's Ethernet interface. (On the Cisco uBR925 cable access router, this pool also applies to the PC connected to the router's USB interface.) The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the router's Ethernet interface. The DHCP lease period is 1 day.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default operations mode of **client**.

Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the cable interface, so that all traffic received and transmitted on the cable interface is sent through the VPN tunnel.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR905Client
!
!
!
!
clock timezone - 0 6
ip subnet-zero
ip tftp source-interface cable-modem0
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool localpool
   import all
   network 192.168.100.0 255.255.255.0
   default-router 192.168.100.1
   lease 1 0 0
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
crypto ipsec client ezvpn hw-client
 peer 188.185.0.5
 group hw-client-groupname key hw-client-password
 mode client
!
!
!
!
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto ipsec client ezvpn hw-client
!
ip classless
no ip http server
no ip http cable-monitor
!
snmp-server packetsize 4096
snmp-server chassis-id
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Client in Client Mode (Cisco 806)

The following example configures a Cisco 806 router as an IPSec client using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the router's Ethernet0 interface. The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the router's Ethernet interface. The DHCP lease period is 1 day.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default operations mode of **client**.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet1 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 806Router
!
!
ip subnet-zero
ip domain-lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 1 0 0
!
!
!
crypto ipsec client ezvpn hw-client
 peer 188.185.0.5
 group hw-client-groupname key hw-client-password
 mode client
```

```
!
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address dhcp
 no cdp enable
 crypto ipsec client ezvpn hw-client
!
ip classless
ip http server
!
!
ip route 0.0.0.0 0.0.0.0 Ethernet1
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local
!
end
```

Cisco Easy VPN Client in Client Mode (Cisco 827)

The following example configures a Cisco 827 router as an IPSec client using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- PPPoE Configuration—The ATM0 interface is configured to support PPPoE connections over the Dialer1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not needed to provide IP addresses to the connected PCs.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **20.0.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default operations mode of **client**.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Dialer1 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

```
version 12.2
```

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
 ip mtu adjust
!
!
!
!
!
!
crypto ipsec client ezvpn hw-client
 group hw-client-groupname key hw-client-password
 mode client
 peer 20.0.0.5
!
!
!
!
!
interface Ethernet0
 ip address 70.0.0.117 255.0.0.0
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
 !
 dsl operating-mode auto
!
interface Dialer1
 ip address 12.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 20.0.0.0 255.0.0.0 12.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
```

```
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Client in Client Mode (Cisco 1700 Series)

The following example configures a Cisco 1700 series router as an IPSec client using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **30.0.0.2** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default operations mode of **client**.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet0 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip dhcp excluded-address 70.0.0.10
!
ip dhcp pool CLIENT
   import all
   network 70.0.0.0 255.255.255.0
   default-router 70.0.0.10
   lease 1 0 0
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
!
crypto ipsec client ezvpn hw-client
```

```
 group hw-client-groupname key hw-client-password
 mode client
 peer 30.0.0.2
!
!
!
!
!
interface Ethernet0
 ip address 50.0.0.10 255.0.0.0
 half-duplex
 crypto ipsec client ezvpn hw-client
!
interface FastEthernet0
 ip address 70.0.0.10 255.0.0.0
 speed auto
!
ip classless
ip route 20.0.0.0 255.0.0.0 Ethernet0
ip route 30.0.0.0 255.0.0.0 Ethernet0
no ip http server
ip pim bidir-enable
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Network Extension Mode Configurations

This section shows the following examples that demonstrate how to configure the Cisco Easy VPN Remote in the network extension mode of operation. Also shown are the VPN remote access server configurations that correspond to these client configurations.

- Cisco Easy VPN Client in Network-Extension Mode (Cisco uBR905/uBR925), page 26
- Cisco Easy VPN Client in Network-Extension Mode (Cisco 806), page 28
- Cisco Easy VPN Client in Network-Extension Mode (Cisco 827), page 29
- Cisco Easy VPN Client in Network-Extension Mode (Cisco 1700 Series), page 31

Cisco Easy VPN Client in Network-Extension Mode (Cisco uBR905/uBR925)

The following example configures a Cisco uBR905 cable access router as an IPSec client, using the Cisco Easy VPN Remote feature in the network extension mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- Routing mode—The **no cable-modem compliant bridge** command places the router in routing mode. IP routing, such as RIPv2, is not activated because the VPN configuration will direct all traffic to the destination point of the VPN tunnel.

- The Ethernet interface is assigned an address in the VPN remote access server's network address space. The **ip route** command directs all traffic for this network space out the cable-modem interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates a Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the **network-extension** mode of operation.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the cable interface, so that all traffic received and transmitted on the cable interface is sent through the VPN tunnel.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR905Client
!
!
!
!
clock timezone - 0 6
ip subnet-zero
ip tftp source-interface cable-modem0
ip dhcp excluded-address 172.168.1.1
!
ip dhcp pool localpool
   import all
   network 172.168.1.0 255.255.255.248
   default-router 172.168.1.1
   lease 1 0 0
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
crypto ipsec client ezvpn hw-client
 peer 188.185.0.5
 group hw-client-groupname key hw-client-password
 mode network-extension
!
!
!
!
!
interface Ethernet0
 ip address 172.168.1.1 255.255.255.248
!
```

```
interface cable-modem0
 no cable-modem compliant bridge
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 0.0.0.0 0.0.0.0 cable-modem0
no ip http server
no ip http cable-monitor
!
snmp-server packetsize 4096
snmp-server chassis-id
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Client in Network-Extension Mode (Cisco 806)

The following example configures a Cisco 806 router as an IPSec client using the Cisco Easy VPN Remote feature. This example shows the following components of the Cisco Easy VPN Remote configuration:

- The Ethernet0 interface is assigned an address in the VPN remote access server's network address space. The **ip route** command directs all traffic for this network space out the Ethernet1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates a Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the **network-extension** mode of operation.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
```

```
service timestamps log uptime
service password-encryption
!
hostname Router
!
!
ip subnet-zero
ip domain-lookup
!
!
ip dhcp excluded-address 172.168.1.1
!
ip dhcp pool localpool
   import all
   network 172.168.1.0 255.255.255.248
   default-router 172.168.1.1
   lease 1 0 0
!
!
crypto ipsec client ezvpn hw-client
 peer 188.185.0.5
 group hw-client-groupname key hw-client-password
 mode network-extension
!
!
interface Ethernet0
 ip address 172.168.1.1 255.255.255.192
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address dhcp
 no cdp enable
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 172.168.0.0 255.255.255.128 Ethernet1
ip http server
!
!
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local
!
end
```

Cisco Easy VPN Client in Network-Extension Mode (Cisco 827)

The following example configures a Cisco 827 router as an IPSec client using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- PPPoE Configuration—The ATM0 interface is configured to support PPPoE connections over the Dialer1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not needed to provide IP addresses to the connected PCs.

- The Ethernet0 interface is assigned an address in the VPN remote access server's network address space. The **ip route** command directs all traffic for this network space out the Dialer1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **20.0.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default operations mode of **network-extension**.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Dialer1 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

Note To use the Cisco Easy VPN Remote (Phase I) feature on Cisco 800 series routers, you must be using Cisco IOS Release 12.2(4)YA, which is not recommended. Cisco recommends using the Phase II version of this feature on Cisco IOS Release 12.2(15)T and later releases.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
 ip mtu adjust
!
!
!
!
!
!
crypto ipsec client ezvpn hw-client
 group hw-client-groupname key hw-client-password
 mode network-extension
 peer 20.0.0.5
!
!
```

```
!
!
!
interface Ethernet0
 ip address 172.168.0.30 255.255.255.192
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
 !
 dsl operating-mode auto
!
interface Dialer1
 ip address 12.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 172.168.0.0 255.255.255.128 Dialer1
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 20.0.0.0 255.0.0.0 12.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Client in Network-Extension Mode (Cisco 1700 Series)

The following example configures a Cisco 1700 series router as an IPSec client using the Cisco Easy VPN Remote feature in the network-extension mode of operation. This example shows the following components of the Cisco Easy VPN Remote configuration:

- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an Cisco Easy VPN Remote configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address **30.0.0.2** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the operations mode of **network-extension**.

  Note If DNS is also configured on the router, the **peer** option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet0 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```
!
```

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
ip dhcp excluded-address 70.0.0.10
!
ip dhcp pool localpool
   import all
   network 70.0.0.0 255.255.255.248
   default-router 70.0.0.10
   lease 1 0 0
!
!
!
crypto ipsec client ezvpn hw-client
 group hw-client-groupname key hw-client-password
 mode network-extension
 peer 30.0.0.2
!
!
!
!
!
interface Ethernet0
 ip address 50.0.0.10 255.0.0.0
 half-duplex
 crypto ipsec client ezvpn hw-client
!
interface FastEthernet0
 ip address 70.0.0.10 255.0.0.0
 speed auto
!
ip classless
ip route 20.0.0.0 255.0.0.0 Ethernet0
ip route 30.0.0.0 255.0.0.0 Ethernet0
no ip http server
ip pim bidir-enable
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

VPN Remote Access Server Configurations

This configuration describes basic VPN Remote Access server configurations that support the Cisco Easy VPN Remote configurations given in the previous sections. For complete information on configuring these servers, see the *VPN Remote Access Enhancements* feature module for Cisco IOS Release 12.2(8)T, available on Cisco.com and the Customer Documentation CD-ROM.

VPN Remote Access Server Without Split Tunneling

The following example shows the VPN remote access server that is the destination peer router for the Cisco Easy VPN Remote network-extension mode configurations shown earlier in this section. In addition to the other IPSec configuration commands, the **crypto isakmp client configuration group hw-client-groupname** defines the attributes for the VPN group that was assigned to the IPSec client router. This includes a matching key value (**hw-client-password**), and the appropriate routing parameters, such as DNS server, for the IPSec clients.

To support the network extension mode of operation, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed out the cable-modem interface to the Cisco Easy VPN Remote. Other **ip route** commands might be needed, depending on your network's topology.

Note This example shows a Cisco uBR925 cable access router, but typically the destination IPsec server will be a router such as a VPN 3000 Concentrator or a Cisco IOS router that supports the VPN Remote Access Enhancements feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network hw-client-groupname local
aaa session-id common
!
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
```

```
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
!
!
crypto map dynmap isakmp authorization list hw-client-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
interface Ethernet0
 ip address 172.168.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.168.0.65 172.168.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.168.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Note The **crypto isakmp client configuration group** command and its subcommands are not officially supported in Cisco IOS Release 12.2(4)YA but are provided only for testing the Cisco Easy VPN Remote feature. These commands will be supported in the 12.2(8)T release that supports the VPN Remote Access Enhancements feature.

VPN Remote Access Server Configuration With Split Tunneling

The following example shows an VPN remote access server configured for a split tunneling configuration with a Cisco Easy VPN Remote. This example is identical to that shown in the "VPN Remote Access Server Without Split Tunneling" section on page 33, except for access list 150, which is

assigned as part of the **crypto isakmp client configuration group hw-client-groupname** command. This access list allows the Cisco Easy VPN Remote to use the server to access one additional subnet that is not part of the VPN tunnel, without compromising the security of the IPsec connection.

To support the network extension mode of operation, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed out the cable-modem interface to the Cisco Easy VPN Remote. Other **ip route** commands might be needed, depending on your network's topology.

Note This example shows a Cisco uBR925 cable access router, but typically the destination IPsec server will be a router such as a VPN 3000 Concentrator or a Cisco IOS router that supports the VPN Remote Access Enhancements feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network hw-client-groupname local
aaa session-id common
!
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
!
!
crypto map dynmap isakmp authorization list hw-client-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
```

```
!
interface Ethernet0
 ip address 172.168.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.168.0.65 172.168.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.168.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.168.0.128 0.0.0.127 any
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Note The **crypto isakmp client configuration group** command and its subcommands are not officially supported in Cisco IOS Release 12.2(4)YA but are provided only for testing the Cisco Easy VPN Remote feature. These commands will be supported in the 12.2(8)T release that supports the VPN Remote Access Enhancements feature.

VPN Remote Access Server Configuration With XAUTH

The following example shows an VPN remote access server configured to support XAUTH authentication with a Cisco Easy VPN Remote. This example is identical to that shown in the "VPN Remote Access Server Configuration With Split Tunneling" section on page 34, except for the following commands that enable and configure XAUTH authentication:

- **aaa authentication login userlist local**—Specifies that the local username database for authentication at login time. You could also specify the use of RADIUS servers by first using the **aaa authentication login userlist group radius** command, and then by specifying the RADIUS servers with the **aaa group server radius** command.
- **username cisco password 7 cisco**—Creates an entry in the local username database for a user with the username of **cisco** and an encrypted password of **cisco**. This command should be repeated for each separate user that will access the server.
- **crypto isakmp xauth timeout**—Specifies the amount of time, in seconds, that the user has to enter the appropriate username and password to authenticate the session.
- **crypto map dynmap client authentication list userlist**—Creates a crypto map named **dynamp** that enables XAUTH authentication.

The following commands, which are also present in the non-XAUTH configurations, are also required for XAUTH use:

- **aaa new-model**—Specifies that the router should use the new AAA authentication commands.

- **aaa authorization network hw-client-groupname local**—Requires authorization for all network-related service requests for users in the group named **hw-client-groupname**, using the local username database.
- **aaa session-id common**—Specifies that a unique and common session ID should be used for AAA sessions.
- **crypto map dynmap isakmp authorization list hw-client-groupname**—Configures the crypto map named **dynmap** to use IKE Shared Secret using the group named **hw-client-groupname**.
- **crypto map dynmap client configuration address respond**—Enables IKE negotiation, accepting requests from any requesting peers.
- **crypto map dynmap 1 ipsec-isakmp dynamic dynmap**—Specifies that IKE should be used to establish the IPSec security associations, using the crypt map named dynmap as the policy template.

Tip This configuration shows the server configured for split tunneling, but XAUTH can also be used with non-split tunnel configurations as well.

Note This example shows a Cisco uBR925 cable access router, but typically the destination IPsec server will be a router such as a VPN 3000 Concentrator or a Cisco IOS router that supports the VPN Remote Access Enhancements feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authentication login userlist local
aaa authorization network hw-client-groupname local
aaa session-id common
!
username cisco password 7 cisco
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
```

```
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
!
!
crypto map dynmap client authentication list userlist
crypto map dynmap isakmp authorization list hw-client-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
interface Ethernet0
 ip address 172.168.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.168.0.65 172.168.0.127
ip classless
ip route 172.168.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.168.0.128 0.0.0.127 any
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Note The **crypto isakmp client configuration group** command and its subcommands are not officially supported in Cisco IOS Release 12.2(4)YA but are provided only for testing the Cisco Easy VPN Remote feature. These commands will be supported in the 12.2(8)T release that supports the VPN Remote Access Enhancements feature.

Command Reference

This section documents new or modified commands to support the Cisco Easy VPN Remote feature. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

This section documents the following commands:

clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN Remote state machine and bring down the Cisco Easy VPN Remote connections on all interfaces, use the **clear crypto ipsec client ezvpn** command in Privileged EXEC mode. If the Cisco Easy VPN Remote connection for a particular interface is configured for auto connect, this command also initiates a new Cisco Easy VPN Remote connection.

clear crypto ipsec client ezvpn

Syntax Description

This command has no keywords or arguments.

Defaults

No default values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

The **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN Remote state machine, bringing down the current Cisco Easy VPN Remote connection and bringing it back up on the interface.

Examples

The following example shows the Cisco Easy VPN Remote state machine being reset.

```
router# clear crypto ipsec client ezvpn
router#
```

Related Commands

Command	Description
crypto ipsec client ezvpn	(global configuration mode) Creates a Cisco Easy VPN Remote configuration.
crypto ipsec client ezvpn	(interface configuration mode) Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec client ezvpn xauth

To respond to a pending VPN authorization request, use the **crypto ipsec client ezvpn xauth** command in Privileged EXEC mode.

crypto ipsec client ezvpn xauth

Syntax Description

This command has no keywords or arguments.

Defaults

No default values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

When making a VPN connection, individual users might also be required to provide authorization information, such as a username or password. When the remote end requires this information, the router displays a message on the router's console instructing the user to enter the **crypto ipsec client ezvpn xauth** command. The user then uses the CLI to give this command and reply to the following prompts to provide the required information.

Note If the user does not respond to the Authentication notification, the message is repeated every ten seconds.

Examples

The following example shows an example of the user being prompted to enter the **crypto ipsec client ezvpn xauth** command. The user then enters the requested information and continues.

```
router#
20:27:39: EZVPN: Pending XAuth Request, Please enter the following command:
20:27:39: EZVPN: crypto ipsec client ezvpn xauth

router# crypto ipsec client ezvpn xauth
Enter Username and Password: userid
Password: ************

router#
```

Related Commands

Command	Description
crypto ipsec client ezvpn	(interface configuration mode) Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec client ezvpn (global configuration)

To create a Cisco Easy VPN Remote configuration and enter the Cisco Easy VPN Remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN Remote configuration, use the **no** form of this command.

crypto ipsec client ezvpn *config-name*

no crypto ipsec client ezvpn *config-name*

Note A separate **crypto ipsec client ezvpn** command exists in interface configuration mode that assigns a Cisco Easy VPN Remote configuration to the interface.

Syntax Description

config-name	Identifies the Cisco Easy VPN Remote configuration with a unique, arbitrary name.

Defaults

Newly created Cisco Easy VPN Remote configurations default to the **client** mode of operation.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN Remote configuration and then enters the Cisco Easy VPN Remote configuration mode, at which point you can enter the following subcommands:

- **group** *group-name* **key** *group-key*—Specifies the group name and key value for the VPN connection.
- **mode** {**client** | **network-extension**}—Specifies the router's VPN mode of operation:
  - The **client** option (default) automatically configures the router for Cisco Easy VPN Remote mode operation, which uses NAT/PAT address translations. When the Cisco Easy VPN Remote configuration is assigned to an interface, the router automatically creates the NAT/PAT and access-list configuration needed for the VPN connection.
  - The **network-extension** option specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the enterprise network's address space.

- **peer** {*ipaddress* | *hostname*}—Sets the peer IP address or hostname for the VPN connection. A hostname can be specified only when the router has a DNS server available for hostname resolution.

Note The Cisco Easy VPN Remote feature attempts to resolve the hostname when the **peer** command is given, not when the VPN tunnel is created. If the hostname cannot be resolved at that time, the **peer** command is not accepted.

- **default**—Sets the following command to its default values.
- **no**—Removes the command or sets it to its default values.

After configuring the Cisco Easy VPN Remote configuration, use the **exit** command to exit the Easy VPN configuration mode and return to global configuration mode.

Note You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN Remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN Remote configuration from the interface before you can delete the configuration.

Examples

The following example shows a Cisco Easy VPN Remote configuration named **telecommuter-client** being created on a Cisco uBR905/uBR925 cable access router and being assigned to cable interface 0:

```
router# config t
router(config)# crypto ipsec client ezvpn telecommuter-client
router(config-crypto-ezvpn)# group telecommute-group key secret-telecommute-key
router(config-crypto-ezvpn)# peer telecommuter-server
router(config-crypto-ezvpn)# mode client
router(config-crypto-ezvpn)# exit
router(config)# interface c0
router(config-if)# crypto ezvpn telecommuter-client
router(config-if)# exit
router(config)#
```

Note Specifying the **mode client** option as shown above is optional because this is default configuration for these options.

The following example shows the Cisco Easy VPN Remote configuration named **telecommuter-client** being removed from the interface and then deleted:

```
router# config t
router(config)# int e1
router(config-if)# no crypto ipsec client ezvpn telecommuter-client
router(config-if)# exit
router(config)# no crypto ipsec client ezvpn telecommuter-client
router(config)#
```

Related Commands

Command	Description
crypto ipsec client ezvpn	(interface configuration mode) Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec client ezvpn (interface configuration)

To assign a Cisco Easy VPN Remote configuration to an interface, use the **crypto ipsec client ezvpn** command in interface configuration mode. To remove the Cisco Easy VPN Remote configuration from the interface, use the **no** form of this command.

crypto ipsec client ezvpn *config-name*

no crypto ipsec client ezvpn *config-name*

Note A separate **crypto ipsec client ezvpn** command exists in global configuration mode that creates a Cisco Easy VPN Remote configuration.

Syntax Description

config-name	Specifies the Cisco Easy VPN Remote configuration to be assigned to the interface.

Defaults

No default values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

The **crypto ipsec client ezvpn** command assigns a Cisco Easy VPN Remote configuration to an interface, enabling the creation of a VPN connection over that interface to the specified VPN peer. If the Cisco Easy VPN Remote configuration is configured for the client mode of operation, this also automatically configures the router for NAT/PAT translation and an associated access list.

The following restrictions apply to the **crypto ipsec client ezvpn** command:

- In Cisco IOS Release 12.2(4)YA, the Cisco Easy VPN Remote feature supports only one tunnel, so the **crypto ipsec client ezvpn** command can be assigned to only one interface. If you attempt to assign it to more than one interface, an error message is displayed. You must use the no form of this command to remove the configuration from the first interface before assigning it to the second interface.
- The **crypto ipsec client ezvpn** command should be assigned to the “outside” interface of the NAT/PAT translation. This command cannot be used on the “inside” NAT/PAT interface. On some platforms, the “inside” or “outside” interfaces are fixed.

For example, on the Cisco uBR905 and Cisco uBR925 cable access routers, the "outside" interface is always the cable interface. On the Cisco 1700 series routers, the FastEthernet interface defaults to being the "inside" interface, so attempting to use the **crypto ipsec client ezvpn** command on the FastEthernet interface displays an error message.

Note You must first use the global configuration version of the **crypto ipsec client ezvpn** command to create a Cisco Easy VPN Remote configuration before assigning it to an interface.

Examples

The following example shows a Cisco Easy VPN Remote configuration named **telecommuter-client** being assigned to the cable interface on a Cisco uBR905/uBR925 cable access router:

```
router# config t
router(config)# interface c0
router(config-if)# crypto ipsec client ezvpn telecommuter-client
router(config-if)# exit
router(config)#
```

The following example first shows an attempt to delete the Cisco Easy VPN Remote configuration named **telecommuter-client**, but the configuration cannot be deleted because it is still assigned to an interface. The configuration is then removed from the interface and then deleted:

```
router# config t
router(config)# no crypto ipsec client ezvpn telecommuter-client
Error: crypto map in use by interface; cannot delete
router(config)# int e1
router(config-if)# no crypto ipsec client ezvpn telecommuter-client
router(config-if)# exit
router(config)# no crypto ipsec client ezvpn telecommuter-client
router(config)#
```

The following example shows an attempt to assign a Cisco Easy VPN Remote configuration to more than one interface. This fails because the Cisco Easy VPN Remote feature supports only one tunnel:

```
router# config t
router(config)# int Ethernet0
router(config-if)# crypto ipsec client ezvpn telecommuter-client
router(config-if)# int Serial0
router(config-if)# crypto ipsec client ezvpn telecommuter-client
Error:Crypto EZVPN currently supports only one tunnel
router(config-if)# exit
router(config)#
```

The following example shows an attempt on a Cisco 1700 series router to assign a Cisco Easy VPN Remote configuration named **telecommuter-client** to the FastEthernet interface. This fails because the FastEthernet interface defaults to being the "inside" interface for the NAT/PAT translation:

```
router-1700# config t
router-1700(config)# int FastEthernet0
router-1700(config-if)# crypto ipsec client ezvpn telecommuter-client
Error:Crypto EZVPN not supported on interface FastEthernet0
router-1700(config-if)# exit
router-1700(config)#
```

Related Commands

Command	Description
crypto ipsec client ezvpn	(global configuration mode) Creates and modifies a Cisco Easy VPN Remote configuration.

show crypto ipsec client ezvpn

To display the Cisco Easy VPN Remote configuration, use the **show crypto ipsec client ezvpn** command in Privileged EXEC mode.

show crypto ipsec client ezvpn

Syntax Description

This command has no keywords or arguments.

Defaults

No default values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Examples

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active VPN connection when the router is in client mode:

```
router# show crypto ipsec client ezvpn
Current State: IPSEC ACTIVE
Last Event: SOCKET UP
Address: 198.1.1.89
Mask: 255.255.255.0
DNS Primary: 198.1.1.250
DNS Secondary: 198.1.1.251
NBMS/WINS Primary: 198.1.1.252
NBMS/WINS Secondary: 198.1.1.253
Default Domain: cisco.com
router#
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active VPN connection when the router is in network-extension mode:

```
router# show crypto ipsec client ezvpn
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 30.0.0.53
Mask: 255.255.255.255
Split Tunnel List: 1
       Address    : 30.100.0.0
       Mask       : 255.255.255.128
       Protocol   : 0x0
       Source Port: 0
```

```
       Dest Port  : 0
router#
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an inactive VPN connection:

```
router# show crypto ipsec client ezvpn
Current State: IDLE
Last Event: REMOVE INTERFACE CFG
router#
```

Table 1 describes the fields shown by the **show crypto ipsec client ezvpn** command:

Table 1 show crypto ipsec client ezvpn Field Descriptions

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the WAN interface.
Mask	Displays the subnet mask used for the outside WAN interface.
DNS Primary	Displays the primary DNS server provided by the DHCP server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.
Domain Name	Displays the domain name provided by the DHCP server.
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Related Commands

Command	Description
show crypto ipsec transform	Displays the specific configuration for one or all transformation sets.

show tech-support

To display general information about the router when reporting a problem to Cisco technical support, use the **show tech-support** command in Privileged EXEC mode.

show tech-support [**page**] [**password**] [**ipmulticast** | **rsvp**]

Syntax Description

page	Pages the output of the command so that it is displayed one screen at a time
password	Displays passwords in the configuration file
ipmulticast	Displays the IP multicast related information by the **show ip pim**, **show ip igmp**, **show ip mroute**, and other IP multicast **show** commands.
rsvp	Displays the IP RSVP related information that is generated by the different **show ip rsvp** commands.

Defaults

Does not display passwords and does not page the output.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0 T	This command was introduced for the Cisco 1700 series router.
12.0 T	This command was introduced for the Cisco 800 series router.
12.1(3a)XL	This command was introduced for the Cisco uBR905 cable access router.
12.1(3)T	Encryption module show commands added for the Cisco 1700 series routers.
12.2(2)XA1	This command was introduced for the Cisco uBR925 cable access router.
12.2(4)YA	This command was enhanced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers by adding the output of Cisco Easy VPN, IPSec, access list, and NAT/PAT **show** commands.
12.2(13)T	Support for Cisco Easy VPN commands was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

The **show tech-support** command displays a large amount of configuration, run-time status, and other information about the router for troubleshooting problems. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command automatically displays the output of a number of different **show** commands. The exact output depends on the platform, configuration, and type of protocols being used. Typically, the output includes the output from the following commands, depending on platform:

Configuration Information

- **show version**

- **show runningconfig**

Run-time State Information

- **show stacks**
- **show interfaces**
- **show controllers**
- **show process memory**
- **show process cpu**
- **show process cpu history**
- **show controller c0 mac state**

Voice Port Information

- **show voice port**
- **show dialpeer voice**
- **show gateway**
- **show call active voice**
- **show call history voice**

Memory Information

- **show region**
- **show buffers**

Cisco Easy VPN Configuration Information

- **show crypto ipsec client ezvpn**
- **show ip nat statistics**
- **show ip nat translations**
- **show crypto map**
- **show access-list**
- **show crypto isakmp policy**
- **show crypto ipsec transform**
- **show crypto isakmp sa**
- **show crypto engine connection active**
- **show crypto ipsec sa**

Tip Depending on the platform and configuration, the output from the **show tech-support** command can easily exceed the buffers found in most communications programs. To capture this output so it can be sent to Cisco TAC, use a Telnet program that allows you to capture the output directly to disk.

Examples

The following shows how to give the **show tech-support** command:

```
Router# show tech-support
```

Related Commands

Command	Description
show running-config	Displays the current run-time configuration.
show startup-config	Displays the configuration that was used to initially configure the CMTS at system startup.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

debug crypto ipsec client ezvpn

To display information showing the configuration and implementation of the Cisco Easy VPN Remote feature, use the **debug crypto ipsec client ezvpn** command in privileged EXEC mode. To turn off debugging of the Cisco Easy VPN Remote feature, use the **no** form of this command.

debug crypto ipsec client ezvpn

no debug crypto ipsec client ezvpn

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for the Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers, the Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	Support was added to the Cisco IOS Release 12.2 T train for Cisco 1700 series routers, and the Cisco uBR905 and Cisco uBR925 cable access routers.

Usage Guidelines

To force the Cisco Easy VPN Remote feature to reestablish the VPN connections, use the **clear crypto sa** and **clear crypto isakmp** commands to delete the IPsec security associations and IKE connections, respectively.

Examples

The following example shows debugging of the Cisco Easy VPN Remote feature being turned on, as well as typical debugging messages that appear when the VPN tunnel is created:

```
router# debug crypto ipsec client ezvpn
EzVPN debugging is on
router#
3d17h: EZVPN: New State: READY
3d17h: EZVPN: Current State: READY
3d17h: EZVPN: Event: MODE_CONFIG_REPLY
3d17h: ezvpn_mode_config
3d17h: ezvpn_parse_mode_config_msg
3d17h: EZVPN: Attributes sent in message:
3d17h:         DNS Primary: 172.168.0.250
3d17h:         DNS Secondary: 172.168.0.251
3d17h:         NBMS/WINS Primary: 172.168.0.252
3d17h:         NBMS/WINS Secondary: 172.168.0.253
3d17h:         Default Domain: cisco.com
3d17h: EZVPN: New State: SS_OPEN
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: SOCKET_READY
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
```

```
3d17h: EZVPN: Event: SOCKET_READY
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: MTU_CHANGED
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: SOCKET_UP
3d17h: EZVPN: New State: IPSEC_ACTIVE
3d17h: EZVPN: Current State: IPSEC_ACTIVE
3d17h: EZVPN: Event: MTU_CHANGED
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: IPSEC_ACTIVE
3d17h: EZVPN: Event: SOCKET_UP
```

The following example shows the typical display for a VPN tunnel that is reset with the **clear crypto ipsec client ezvpn** command:

```
3d17h: EZVPN: Current State: READY
3d17h: EZVPN: Event: RESET
3d17h: ezvpn_reconnect_request
3d17h: ezvpn_close
3d17h: ezvpn_connect_request
3d17h: EZVPN: New State: READY
3d17h: EZVPN: Current State: READY
3d17h: EZVPN: Event: MODE_CONFIG_REPLY
3d17h: ezvpn_mode_config
3d17h: ezvpn_parse_mode_config_msg
3d17h: EZVPN: Attributes sent in message:
3d17h:         DNS Primary: 172.168.0.250
3d17h:         DNS Secondary: 172.168.0.251
3d17h:         NBMS/WINS Primary: 172.168.0.252
3d17h:         NBMS/WINS Secondary: 172.168.0.253
3d17h:         Split Tunnel List: 1
3d17h:               Address    : 172.168.0.128
3d17h:               Mask       : 255.255.255.128
3d17h:               Protocol   : 0x0
3d17h:               Source Port: 0
3d17h:               Dest Port  : 0
3d17h:         Split Tunnel List: 2
3d17h:               Address    : 172.168.1.128
3d17h:               Mask       : 255.255.255.128
3d17h:               Protocol   : 0x0
3d17h:               Source Port: 0
3d17h:               Dest Port  : 0
3d17h:         Default Domain: cisco.com
3d17h: ezvpn_nat_config
3d17h: EZVPN: New State: SS_OPEN
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: SOCKET_READY
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: SOCKET_READY
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: MTU_CHANGED
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: SS_OPEN
3d17h: EZVPN: Event: SOCKET_UP
3d17h: EZVPN: New State: IPSEC_ACTIVE
3d17h: EZVPN: Current State: IPSEC_ACTIVE
3d17h: EZVPN: Event: MTU_CHANGED
3d17h: EZVPN: No state change
3d17h: EZVPN: Current State: IPSEC_ACTIVE
3d17h: EZVPN: Event: SOCKET_UP
```

The following example shows the typical display for a VPN tunnel that is removed from the interface with the no **crypto ipsec client ezvpn** command:

```
4d16h: EZVPN: Current State: IPSEC ACTIVE
4d16h: EZVPN: Event: REMOVE INTERFACE CFG
4d16h: ezvpn_close_and_remove
4d16h: ezvpn_close
4d16h: ezvpn_remove
4d16h: EZVPN: New State: IDLE
```

Related Commands

Command	Description
debug crypto ipsec	Displays debugging messages for generic IPsec events.
debug crypto isakmp	Displays debugging messages for Internet Key Exchange (IKE) events.

Glossary

AAA—authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

aggressive mode—This mode eliminates several steps during IKE authentication negotiation (phase 1) between two or more IPSec peers. Aggressive mode is faster than main mode, but not as secure.

authentication, authorization, and accounting—See AAA.

authorization—The method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. All authorization methods must be defined through AAA.

IKE—A key management protocol standard which is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.

CA—certificate authority. A certificate authority (CA) is an entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Certificates generally include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

certification authority—See CA.

Internet Key Exchange—See IKE.

IP Security Protocol—See IPSec.

IPSec—IP Security Protocol. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

main mode—This mode ensures the highest level of security when two or more IPSec peers are negotiating IKE authentication (phase 1). It requires more processing time than aggressive mode.

Management Information Base—See MIB.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (MIP). The value of a MIB object can be changed or

retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

peer—A router or device that participates as an endpoint in IPSec and IKE.

pre-shared key—A pre-shared key is a shared, secret key that uses IKE for authentication.

QoS—Quality of Service. QoS refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

RADIUS—Remote Authentication Dial-In User Service. A distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Remote Authentication Dial-In User Service—See RADIUS.

SA—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

security association—See SA.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Virtual Private Network—See VPN.

VPN—virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.