



# L2TP Security

---

## Feature History for L2TP Security

Release	Modification
12.2(4)T	This feature was introduced.
12.2(4)T3	Support for the Cisco 7500 series routers was added.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

This document describes the L2TP Security feature in Cisco IOS Release 12.2(11)T. It includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 5](#)
- [Configuration Examples, page 14](#)
- [Command Reference, page 17](#)



---

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

Copyright © 2002–2005 Cisco Systems, Inc. All rights reserved.

# Feature Overview

The L2TP Security feature provides enhanced security for tunneled PPP frames between the Layer 2 Transport Protocol (L2TP) access concentrator (LAC) and the L2TP network server (LNS). Previous releases of the Cisco IOS software provided only a one-time, optional mutual authentication during tunnel setup with no authentication of subsequent data packets or control messages. In situations where the L2TP is used to tunnel PPP sessions over an untrusted infrastructure such as the Internet, the security attributes of L2TP and PPP are inadequate. PPP provides no protection of the L2TP tunnel, and current PPP encryption protocols provide inadequate key management and no authentication or integrity mechanisms. The L2TP Security feature allows the robust security features of IP Security (IPSec) to protect the L2TP tunnel and the PPP sessions within the tunnel. In addition, the L2TP Security feature provides built-in keepalives and standardized interfaces for user authentication and accounting to authentication, authorization, and accounting (AAA) servers.

The deployment of Microsoft Windows 2000 demands the integration of IPSec with L2TP because this is the default virtual private dialup network (VPDN) networking scenario. This integration of protocols is also used for LAN-to-LAN VPDN connections in Microsoft Windows 2000. The L2TP Security feature provides integration of IPSec with L2TP in a solution that is scalable to large networks with minimal configuration.

## Benefits

The enhanced security provided by the L2TP Security feature increases the integrity and confidentiality of tunneled PPP sessions within a standardized, well deployed Layer 2 tunneling solution. The robust security features of IPSec and Internet Key Exchange (IKE) include confidentiality, integrity checking, replay protection, authentication and key management. Traditional routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP) will run transparently because a real PPP interface is associated with the secure tunnel. Additional benefits include built in keepalives and standardized interfaces for user authentication and accounting to AAA servers, interface statistics, standardized MIBs, and multiprotocol support.

## Related Features and Technologies

- L2TP Large-Scale Dial-Out
- Timer and Retry Enhancements for L2TP and L2F
- VPDN Group Session Limiting

## Related Documents

- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2

# Supported Platforms

- Cisco 806
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2691
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3700 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5300
- Cisco AS5400
- Cisco AS5800
- Cisco IGX 8400 URM

## Determining Platform Support Through Cisco Feature Navigator

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

Cisco 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. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco 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](mailto: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 found at this URL:

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

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

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

**Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

**Standards**

No new or modified standards are supported by this feature.

**MIBs**

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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](mailto: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 found at this URL:

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

**RFCs**

- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 2401, *Security Architecture for the Internet Protocol (IPSec)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2637, *Point to Point Tunneling Protocol (PPTP)*
- RFC 2661, *Layer Two Transport Protocol (L2TP)*
- RFC 3193, *Securing L2TP Using IPSec*

## Prerequisites

The interface between the LAC and LNS must be configured for IP and must support IPSec.

To use the L2TP Security feature for client-initiated dial-in using compulsory tunneling, the interface between the client and the LAC must support PPP.

To use the L2TP Security feature for client-initiated dial-in using voluntary tunneling, the client software must support L2TP and IPSec. This is the default VPDN networking scenario in Microsoft Windows 2000.

## Configuration Tasks

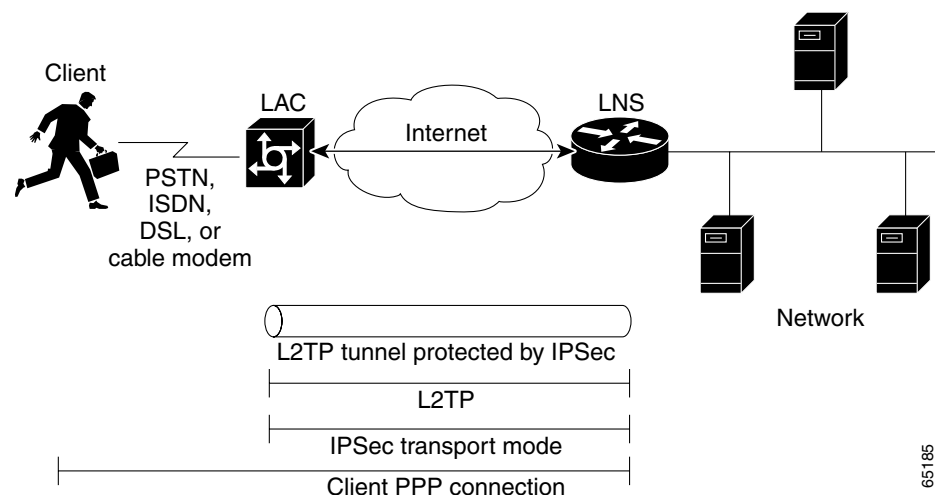
See the following sections for configuration tasks for the L2TP Security feature. Each task in the list is identified as either required or optional:

- [Configuring NAS-Initiated VPDN Tunneling with L2TP Security](#) (optional)
- [Configuring Client-Initiated VPDN Tunneling with L2TP Security](#) (optional)

## Configuring NAS-Initiated VPDN Tunneling with L2TP Security

In the NAS-initiated (compulsory) tunneling scenario depicted in [Figure 1](#), the client connects to the LAC through a media that supports PPP, such as a dialup modem, DSL, ISDN, or a cable modem. If the connection from the client to the LAC is considered secure such as a modem, ISDN or a DSL connection the client may choose not to provide additional security. The PPP session is securely tunneled from the LAC to the LNS without any required knowledge or interaction by the client.

**Figure 1** NAS-Initiated Tunneling



To configure the L2TP Security feature for compulsory tunneling, perform the tasks described in the following sections to configure the client, LAC, and LNS:

- [Configuring the Client](#) (required)
- [Configuring the LAC](#) (required)
- [Configuring the LNS](#) (required)

### Configuring the Client

To use the L2TP Security feature for NAS-initiated dial-in using compulsory tunneling, configure the interface between the client and the LAC for PPP. For more information on configuring PPP on the client, refer to the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

## Configuring the LAC

To configure the LAC to use the L2TP Security feature, perform the required tasks described in the following sections:

- [Configuring the Interface Between the LAC and the LNS](#) (required)
- [Configuring IPSec Protection of a L2TP Tunnel at the LAC](#) (required)
- [Creating the Security Profile at the LAC](#) (required)

## Configuring the Interface Between the LAC and the LNS

To configure the interface between the LAC and the LNS, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>username</b> <i>username</i> <b>password</b> <i>secret</i>	Establishes a username-based authentication system for L2TP tunnel authentication at the LAC.
Step 2	Router(config)# <b>username</b> <i>username</i> <b>password</b> <i>secret</i>	Establishes a username-based authentication system for L2TP tunnel authentication at the LNS.
Step 3	Router(config)# <b>vpdn enable</b>	Enables VPDN on the router.
Step 4	Router(config)# <b>no vpdn logging</b>	Disables the logging of VPDN events.

## Configuring IPSec Protection of a L2TP Tunnel at the LAC


To configure a VPDN group to tunnel PPP sessions with IPSec protection, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>vpdn-group</b> <i>name</i>	Enters VPDN group configuration mode and associates a VPDN group to a VPDN profile.
Step 2	Router(config-vpdn)# <b>request-dialin</b>	Enters VPDN request-dialin configuration submode, configures the LAC to request L2TP tunnels to the LNS, and specifies a VPDN subgroup.
Step 3	Router(config-vpdn-req-in)# <b>protocol</b> <i>l2tp</i>	Specifies L2TP as the tunneling protocol that the VPDN subgroup will use.
Step 4	Router(config-vpdn-req-in)# <b>domain</b> <i>name</i>	Requests that PPP calls from a specific domain name be tunneled. The request-dialin VPDN subgroup can be configured to tunnel calls from multiple Domain Name System numbers and domain names.
Step 5	Router(config-vpdn-req-in)# <b>exit</b>	Exits VPDN request-dialin configuration submode.
Step 6	Router(config-vpdn)# <b>initiate-to ip</b> <i>ip-address</i>	Specifies the IP address to which the LAC will tunnel.
Step 7	Router(config-vpdn)# <b>local name</b> <i>name</i>	Specifies a local host name that the tunnel will use to identify itself.

	Command	Purpose
Step 8	Router(config-vpdn)# <b>l2tp security crypto-profile</b> <i>profile-name</i> [ <b>keep-sa</b> ]	<p>Enables the VPDN group to be protected by IPsec.</p> <ul style="list-style-type: none"> <li><i>profile-name</i>—The name of the crypto profile to be used for IPsec protection of tunneled PPP sessions. The <i>profile-name</i> must match that of a profile configured using the <b>crypto-map</b> command.</li> <li><b>keep-sa</b>—This keyword is used to control the destruction of IPsec security associations (SAs) upon tunnel teardown. By default, any IPsec phase 2 SAs and IKE phase 1 SAs are destroyed when the L2TP tunnel is torn down. Using the <b>keep-sa</b> keyword prevents the destruction of IKE phase 1 SAs.</li> </ul>
Step 9	Router(config-vpdn)# <b>l2tp tunnel password</b> <i>password</i>	Sets the password that the router will use to authenticate the tunnel.

### Creating the Security Profile at the LAC

To create an IKE policy and a crypto profile configuration associated with the VPDN group, you must first configure phase 1 ISAKMP policy and an IPsec transform set. For more information on configuring phase 1 ISAKMP policies and IPsec transform, sets refer to the *Cisco IOS Security Configuration Guide*, Release 12.2. Once the phase 1 ISAKMP policy and an IPsec transform set have been configured, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>crypto map</b> <i>map-name</i> <i>seq-num</i> <b>ipsec-isakmp profile</b> <i>profile-name</i>	<p>Enters crypto map configuration mode and creates a crypto profile to be used as a configuration template for dynamically created crypto maps.</p> <p> <b>Note</b> The <b>set peer</b> and <b>match address</b> commands are ignored by crypto profiles and should not be configured in the crypto map definition.</p>
Step 2	Router(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name</i> [ <i>transform-set-name2</i> ... <i>transform-set-name6</i> ]	Specifies which transform sets can be used with the crypto map entry.
Step 3	Router(config-crypto-map)# <b>exit</b>	Returns to global configuration mode.
Step 4	Router(config)# <b>interface fastethernet</b> <i>slot/port</i>	Enters interface configuration mode and selects a particular Fast Ethernet interface for configuration.
Step 5	Router(config-if)# <b>ip address</b> <i>ip-address</i> <i>mask</i>	Sets a primary IP address for the interface.
Step 6	Router(config-if)# <b>crypto map</b> <i>map-name</i>	Associates the crypto map with the interface.



## Configuring the LNS

To configure the LNS to use the L2TP Security feature, perform the required tasks described in the following sections:

- [Configuring the Interface Between the LNS and the LAC](#) (required)
- [Configuring IPSec Protection of an L2TP Tunnel at the LNS](#) (required)
- [Creating the Security Profile at the LNS](#) (required)

### Configuring the Interface Between the LNS and the LAC

To configure the interface between the LNS and the LAC, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>username</b> <i>username</i> <b>password</b> <i>secret</i>	Establishes a username-based authentication system for Challenge Handshake Authentication Protocol (CHAP) authentication of the client.
Step 2	Router(config)# <b>username</b> <i>username</i> <b>password</b> <i>secret</i>	Establishes a username-based authentication system for L2TP tunnel authentication at the LAC.
Step 3	Router(config)# <b>username</b> <i>username</i> <b>password</b> <i>secret</i>	Establishes a username-based authentication system for L2TP tunnel authentication at the LNS.
Step 4	Router(config)# <b>ip</b> <b>address</b> <b>pool</b> <i>local</i>	Enables address pooling to supply IP addresses to the client.
Step 5	Router(config)# <b>vpdn</b> <b>enable</b>	Enables VPDN on the router.

### Configuring IPSec Protection of an L2TP Tunnel at the LNS

To configure a VPDN group to tunnel PPP sessions with IPSec protection, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>vpdn-group</b> <i>name</i>	Enters VPDN group configuration mode and associates a VPDN group to a VPDN profile.
Step 2	Router(config-vpdn)# <b>accept</b> <b>dialin</b>	Enters VPDN accept-dialin configuration mode, configures the LNS to accept tunneled PPP connections from a LAC, and specifies a VPDN subgroup.
Step 3	Router(config-vpdn-acc-in)# <b>protocol</b> <b>l2tp</b>	Specifies L2TP as the tunneling protocol the VPDN subgroup will use.
Step 4	Router(config-vpdn-acc-in)# <b>virtual-template</b> <i>template-number</i>	Specifies which virtual template will be used to clone virtual access interfaces.
Step 5	Router(config-vpdn-acc-in)# <b>exit</b>	Returns to VPDN group configuration mode.
Step 6	Router(config-vpdn)# <b>terminate-from</b> <b>hostname</b> <i>host-name</i>	Specifies the host name of the remote LAC that is required to accept a VPDN tunnel.

	Command	Purpose
Step 7	Router(config-vpdn)# <b>lcp renegotiation</b> {always   on-mismatch}	Allows the LNS to renegotiate the Link Control Protocol (LCP).
Step 8	Router(config-vpdn-acc-in)# <b>l2tp security crypto-profile</b> profile-name [keep-sa]	Enables the VPDN group to be protected by IPsec. <ul style="list-style-type: none"> <li><i>profile-name</i>—The name of the crypto profile to be used for IPsec protection of tunneled PPP sessions. The <i>profile-name</i> must match that of a profile configured using the <b>crypto-map</b> command.</li> <li><b>keep-sa</b>—This keyword is used to control the destruction of IPsec security associations (SAs) upon tunnel teardown. By default, any IPsec phase 2 SAs and IKE phase 1 SAs are destroyed when the L2TP tunnel is torn down. Using the <b>keep-sa</b> keyword prevents the destruction of IKE phase 1 SAs.</li> </ul>

### Creating the Security Profile at the LNS

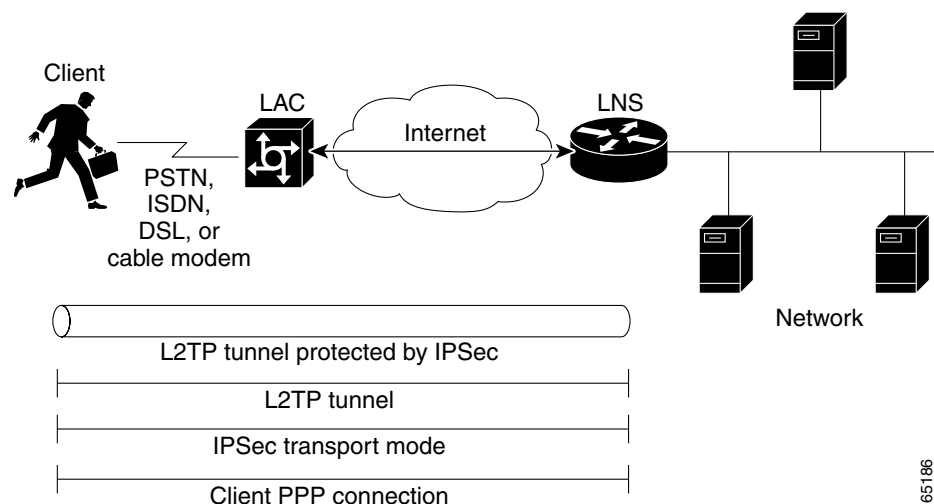
To create an IKE policy and a crypto profile configuration associated with the VPDN group, you must first configure phase 1 ISAKMP policy and an IPsec transform set. For more information on configuring phase 1 ISAKMP policies and IPsec transform, sets refer to the *Cisco IOS Security Configuration Guide*, Release 12.2. Once the phase 1 ISAKMP policy and an IPsec transform set have been configured, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>crypto map</b> map-name seq-num ipsec-isakmp profile profile-name	Enters crypto map configuration mode and creates a crypto profile to be used as a configuration template for dynamically created crypto maps.
Step 2	Router(config-crypto-map)# <b>set transform-set</b> transform-set-name [transform-set-name2...transform-set-name6]	Specifies which transform sets can be used with the crypto map entry.
Step 3	Router(config-crypto-map)# <b>exit</b>	Returns to global configuration mode.
Step 4	Router(config)# <b>interface fastethernet</b> slot/port	Enters interface configuration mode and selects a particular Fast Ethernet interface for configuration.
Step 5	Router(config-if)# <b>ip address</b> ip-address mask	Sets a primary IP address for the interface.
Step 6	Router(config-if)# <b>speed</b> {10   100   auto}	Configures the speed for a Fast Ethernet interface.
Step 7	Router(config-if)# <b>half-duplex</b>	Specifies half-duplex mode.
Step 8	Router(config-if)# <b>crypto map</b> map-name	Associates the crypto map with the interface.

## Configuring Client-Initiated VPDN Tunneling with L2TP Security

In the client-initiated (voluntary) tunneling scenario depicted in [Figure 2](#), the client initiates an L2TP tunnel to the LNS without the intermediate NAS participating in tunnel negotiation or establishment. The client must manage the software that initiates the tunnel. Microsoft Windows 2000 supports this VPDN scenario. In this scenario, extended services processor (ESP) with authentication must always be used.

**Figure 2** Client-Initiated Tunneling



To configure the L2TP Security feature for voluntary tunneling, you must configure the LNS to interface with the LAC by performing the tasks described in the “[Configuring the Interface Between the LNS and the LAC](#)” section.

In addition, perform the tasks in the following sections, which are unique to configuring the NAS for client-initiated dial-in using voluntary tunneling:

- [Configuring IPsec Protection of a VPDN Session at the LNS](#) (required)
- [Creating the Security Profile at the LNS](#) (required)

### Configuring IPsec Protection of a VPDN Session at the LNS

To configure a VPDN group to tunnel PPP sessions with IPsec protection, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	<code>Router(config)# vpdn-group name</code>	Enters VPDN group configuration mode and associates a VPDN group to a VPDN profile.
<b>Step 2</b>	<code>Router(config-vpdn)# accept dialin</code>	Enters VPDN accept-dialin configurative mode, configures the LNS to accept tunneled PPP connections from a LAC, and specifies a VPDN subgroup.
<b>Step 3</b>	<code>Router(config-vpdn-acc-in)# protocol l2tp</code>	Specifies L2TP as the tunneling protocol the VPDN subgroup will use.

	Command	Purpose
Step 4	Router(config-vpdn-acc-in)# <b>virtual-template</b> <i>template-number</i>	Specifies which virtual template will be used to clone virtual access interfaces.
Step 5	Router(config-vpdn-acc-in)# <b>l2tp security</b> <b>crypto-profile</b> <i>profile-name</i> [ <b>keep-sa</b> ]	Enables the VPDN group to be protected by IPSec. <ul style="list-style-type: none"> <li><i>profile-name</i>—The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions. The <i>profile-name</i> must match that of a profile configured using the <b>crypto-map</b> command.</li> <li><b>keep-sa</b>—This keyword</li> </ul>
Step 6	Router(config-vpdn)# <b>no l2tp tunnel authentication</b>	Disables L2TP tunnel authentication.
Step 7	Router(config-vpdn)# <b>lcp renegotiation</b> { <b>always</b>   <b>on-mismatch</b> }	Allows the LNS to renegotiate the LCP.
Step 8	Router(config-vpdn)# <b>ip pmtu</b>	Allows L2TP tunnels to participate in path maximum transmission unit (MTU) discovery.

### Creating the Security Profile at the LNS

To create an IKE policy and a crypto profile configuration associated with the VPDN group, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>crypto ipsec transform-set</b> <i>transform-set-name transform1</i> [ <i>transform2</i> ] [ <i>transform3</i> ]	Enters crypto transform configuration mode and defines a transform set.  There are complex rules defining which entries you can use for the <i>transform</i> arguments. For more information, refer to the <b>crypto ipsec transform-set</b> command description or the table of allowed transform combinations.
Step 2	Router(config-crypto-trans)# <b>crypto map</b> <i>map-name</i> <i>seq-num ipsec-isakmp profile profile-name</i>	Enters crypto map configuration mode and creates a crypto profile to be used as a configuration template for dynamically created crypto maps.
Step 3	Router(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name</i> [ <i>transform-set-name2</i> ... <i>transform-set-name6</i> ]	Specifies which transform sets can be used with the crypto map entry.
Step 4	Router(config-crypto-map)# <b>set security-association</b> <b>lifetime</b> { <b>seconds</b> <i>seconds</i>   <b>kilobytes</b> <i>kilobytes</i> }	Overrides the global lifetime value for a particular crypto map entry. The global lifetime value is used when negotiating IPSec security associations.
Step 5	Router(config-crypto-map)# <b>exit</b>	Returns to global configuration mode.
Step 6	Router(config)# <b>interface fastethernet</b> <i>slot/port</i>	Enters interface configuration mode and selects a particular Fast Ethernet interface for configuration.
Step 7	Router(config-if)# <b>ip address</b> <i>ip-address mask</i>	Sets a primary IP address for the interface.
Step 8	Router(config-if)# <b>speed</b> { <b>10</b>   <b>100</b>   <b>auto</b> }	Configures the speed for a Fast Ethernet interface.

	Command	Purpose
Step 9	Router(config-if)# <b>half-duplex</b>	Specifies half-duplex mode.
Step 10	Router(config-if)# <b>crypto map</b> <i>map-name</i>	Associates the crypto map with the interface.

## Verifying Session Establishment

To verify the establishment and security of an L2TP tunnel, perform the following steps:

- Step 1** Enable the **debug crypto socket** and **debug vpdn l2x-events** commands. The **crypto socket messages** command allows you to view socket messages and verify that the socket is created and moved to the active state. The **vpdn l2x-events** command tracks incoming and outgoing L2TP packets.

```
router# debug crypto socket
router# debug vpdn l2x-events
*Mar 1 00:56:46.959:CRYPTO_SS(L2X Security):Passive open, socket info:local
10.0.0.13/1701, remote 10.0.0.12/1701, prot 17, ifc Fa0/0
*Mar 1 00:56:47.291:L2TP:I SCCRQ from ebooth02 tnl 5107
*Mar 1 00:56:47.295:L2X:Requested security for socket, UDP socket info:local
10.0.0.13(1701), remote 10.0.0.12(1701)
*Mar 1 00:56:47.295:Tnl 13582 L2TP:Got a challenge in SCCRQ, ebooth02
*Mar 1 00:56:47.295:Tnl 13582 L2TP:New tunnel created for remote ebooth02, address
10.0.0.12
*Mar 1 00:56:47.295:Tnl 13582 L2TP:O SCCRQ to ebooth02 tnlid 5107
*Mar 1 00:56:47.295:Tnl 13582 L2TP:Control channel retransmit delay set to 1 seconds
*Mar 1 00:56:47.299:Tnl 13582 L2TP:Tunnel state change from idle to wait-ctl-reply
*Mar 1 00:56:47.299:CRYPTO_SS(L2X Security):Completed binding of application to socket
```

- Step 2** Use the **show crypto map tag** *crypto-map-name* command to verify that a crypto map was dynamically created for the L2TP tunnel.

```
router# show crypto map tag l2tpsec
Crypto Map "l2tpsec" 10 ipsec-isakmp
No matching address list set.
Current peer:0.0.0.0
Security association lifetime:4608000 kilobytes/3600 seconds
PFS (Y/N):N
Transform sets={ esp, }

Crypto Map "l2tpsec" 20 ipsec-isakmp
Peer = 10.0.0.13
Extended IP access list
access-list permit udp host 10.0.0.12 port = 1701 host 10.0.0.13 port = 1701
Current peer:10.0.0.13
Security association lifetime:4608000 kilobytes/3600 seconds
PFS (Y/N):N
Transform sets={ esp, }
Interfaces using crypto map l2tpsec:
FastEthernet0/0
```

- Step 3** To verify that packets are being encrypted/decrypted for the secure tunnel, use the **show crypto engine connections active** command.

```
router#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	10.0.0.13	set	HMAC_SHA+DES_56_CB	0	0
2000	FastEthernet0/0	10.0.0.13	set	HMAC_SHA+DES_56_CB	0	62
2001	FastEthernet0/0	10.0.0.13	set	HMAC_SHA+DES_56_CB	64	0

# Configuration Examples

This section provides the following configuration examples:

- [Configuring IPsec Protection of LAC-Initiated L2TP Tunnels Example](#)
- [Configuring IPsec Protection of Client-Initiated L2TP Tunnels Example](#)

## Configuring IPsec Protection of LAC-Initiated L2TP Tunnels Example

The following example configures L2TP Security on the client, LAC, and LNS for a compulsory tunneling scenario.

### Client Configuration

```
! PPP configuration on the client.
interface Serial11/0
 ip address negotiated
 encapsulation ppp
 clockrate 128000
 no cdp enable
 ppp chap hostname userSerial10@cisco.com
 ppp chap password cisco
```

### LAC Configuration

```
! Passwords for the L2TP tunnel authentication.
username LAC password 0 cisco
username LNS password 0 cisco
!
! VPDN configuration to tunnel users with the domain cisco.com
! to the LNS. This configuration has l2tp tunnel authentication
! enabled.
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.0.0.13
 local name LAC
 l2tp security crypto-profile l2tp keep-sa
 l2tp tunnel password cisco
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.0.0.13
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
! Crypto profile configuration which is bound to the vpdn-group shown above.
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set esp-des-sha-transport
!
interface FastEthernet0/0
 ip address 10.0.0.12 255.255.255.0
 crypto map l2tpsec
```

### LNS Configuration

```
! PPP client username and password needed for CHAP authentication.
username userSerial10@cisco.com password 0 cisco
!
! Passwords for the L2TP tunnel authentication.
username LAC password 0 cisco
username LNS password 0 cisco
!
! Using address pool to assign client an IP address.
ip address-pool local
!
! VPDN configuration.
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
 terminate-from hostname LAC
 lcp renegotiation on-mismatch
 l2tp security crypto-profile l2tp keep-sa
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.0.0.12
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set esp-des-sha-transport
!
interface FastEthernet0/0
 ip address 10.0.0.13 255.255.255.0
 speed 10
 half-duplex
 crypto map l2tpsec
```

## Configuring IPsec Protection of Client-Initiated L2TP Tunnels Example

The following example configures L2TP Security on the LNS for a voluntary tunneling scenario.

### LNS Configuration

```
! PPP client username and password needed for CHAP authentication.
username userSerial10@cisco.com password 0 cisco
! Passwords for the L2TP tunnel authentication.
username LAC password 0 cisco
username LNS password 0 cisco
!
! Using address pool to assign client an IP address.
ip address-pool local
!
! VPDN configuration.
vpdn enable
!
vpdn-group dial-in
  accept-dialin
  protocol l2tp
  virtual-template 1
  l2tp security crypto-profile l2tp
  no l2tp tunnel authentication
ip pmtu
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
mode transport
!
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
  set transform-set esp-des-sha-transport
  set security-association lifetime seconds 120
!
interface FastEthernet0/0
  ip address 10.0.0.13 255.255.255.0
  speed 10
  half-duplex
  crypto map l2tpsec
```



# Command Reference

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

## New Commands

- [ip pmtu](#)
- [l2tp security crypto-profile](#)

## Modified Commands

- [crypto map \(global IPSec\)](#)

# ip pmtu

To enable the discovery of a path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group configuration mode or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

**ip pmtu**

**no ip pmtu**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Path MTU discovery is disabled.

**Command Modes** VPDN group configuration  
Pseudowire class configuration

## Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

## Usage Guidelines

When issued in VPDN group configuration mode, the **ip pmtu** command enables any Layer 2 Tunnel Protocol (L2TP) tunnel associated with the specified virtual private dial-up network (VPDN) group to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Path MTU checks decrease switching performance; therefore this option is disabled by default.

The **ip pmtu** command enables the processing of Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. The MTU of the Layer 2 session is updated according to the MTU information contained in the ICMP unreachable message.

The **ip pmtu** command also enables MTU checking for IP packets that are sent into a Layer 2 session with the Don't Fragment (DF) bit set. If an IP packet is larger than the MTU of the tunnel, the packet is dropped and an ICMP unreachable message is sent. If an IP packet is smaller than the MTU of the tunnel, the DF bit in the packet header is reflected from the inner IP header to the tunnel header.

**Examples**

The following example configures a VPDN group named “dial-in” on an L2TP network server and uses the **ip pmtu** command to specify that L2TP tunnels will participate in path MTU discovery:

```
vpdn-group dial-in
  accept-dialin
  protocol l2tp
  virtual-template 1
  l2tp security crypto-profile l2tp
  no l2tp tunnel authentication
  lcp renegotiation on-mismatch
  ip pmtu
```

The following example shows how to enable the discovery of the path MTU for pseudowires that have been created from the pseudowire class named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip pmtu
```

**Related Commands**

Command	Description
<b>ip dfbit set</b>	Enables the DF bit in the outer Layer 2 tunnel header.
<b>pseudowire-class</b>	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

## l2tp security crypto-profile

To enable a virtual private dialup network (VPDN) group to be protected by IP Security (IPSec), use the **l2tp security crypto-profile** command in VPDN group configuration mode. To disable IPSec security for a VPDN group, use the **no** form of this command.

**l2tp security crypto-profile** *profile-name* [**keep-sa**]

**no l2tp security crypto-profile** *profile-name* [**keep-sa**]

### Syntax Description

<i>profile-name</i>	The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions. The <i>profile-name</i> argument must match that of a profile configured using the <b>crypto map</b> command.
<b>keep-sa</b>	(Optional) Controls the destruction of IPSec security associations (SAs) upon tunnel teardown. By default, any IPSec phase 2 SAs and Internet Key Exchange (IKE) phase 1 SAs are destroyed when the Layer 2 Transport Protocol (L2TP) tunnel is torn down. Using the <b>keep-sa</b> keyword prevents the destruction of IKE phase 1 SAs.

### Defaults

IPSec security is disabled.  
SAs are destroyed on tunnel teardown.

### Command Modes

VPDN group configuration

### Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

### Usage Guidelines

A crypto profile must be configured using the **crypto map** (global IPSec) command before it can be associated with a VPDN group using the **l2tp security crypto-profile** command. Enabling this command for a VPDN group ensures that no L2TP packets will be processed unless they have IPSec protection.

The **keep-sa** keyword can be used to prevent the destruction of IKE phase 1 SAs when the L2TP tunnel between the L2TP access concentrator (LAC) and L2TP network server (LNS) is considered permanent, and the IP addresses of the LAC and LNS rarely change. This option is not useful with short-lived tunnels, such as those generated by client-initiated L2TP tunneling.

**Examples**

The following example configures VPDN group 1, associates it with the crypto profile named l2tp, and prevents the destruction of IKE phase 1 SAs:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.0.0.13
 local name LAC
 l2tp security crypto-profile l2tp keep-sa
```

**Related Commands**

Command	Description
<b>crypto map (global IPsec)</b>	Creates or modifies a crypto map entry or creates a crypto profile that provides a template for configuration of dynamically created crypto maps.

## crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

**crypto map** *map-name seq-num* [**ipsec-manual**]

**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**]  
[**profile** *profile-name*]

**crypto map** *map-name* [**client-accounting-list** *aaalist*]

**no crypto map** *map-name seq-num*



### Note

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

### Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>seq-num</i>	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the “Usage Guidelines” section.
<b>ipsec-manual</b>	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
<b>ipsec-isakmp</b>	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
<b>dynamic</b>	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
<b>discover</b>	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
<b>profile</b>	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
<i>profile-name</i>	(Optional) Name of the crypto profile being created.
<b>client-accounting-list</b>	(Optional) Designates a client accounting list.
<i>aaalist</i>	(Optional) List name.

### Defaults

No crypto maps exist.

Peer discovery is not enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	11.3 T	The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <b>ipsec-manual</b></li> <li>• <b>ipsec-isakmp</b></li> <li>• <b>dynamic</b></li> <li>• <i>dynamic-map-name</i></li> </ul>
	12.0(5)T	The <b>discover</b> keyword was added to support Tunnel Endpoint Discovery (TED).
	12.2(4)T	The <b>profile</b> <i>profile-name</i> keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
	12.2(11)T	Support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
	12.2(15)T	The <b>client-accounting-list</b> keyword and <i>aaalist</i> argument were added.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

### Usage Guidelines

Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

### Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used or managed (or what the keys are, if IKE is not used)

### Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

### Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named “mymap” is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

### Dynamic Crypto Maps

Refer to the “Usage Guidelines” section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

### TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.



#### Note

---

TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

---



### Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the Layer 2 Transport Protocol (L2TP) Security feature. The relevant SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.



#### Note

The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

### Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcbafedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPsec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPsec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPsec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPsec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPsec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
```

```

crypto map mymap 20 ipsec-isakmp
 match address 102
  set transform-set my_t_set1 my_t_set2
  set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
  set transform-set my_t_set1 my_t_set2 my_t_set3

```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

### Related Commands

Command	Description
<b>crypto dynamic-map</b>	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
<b>crypto isakmp profile</b>	Audits IPSec user sessions.
<b>crypto map (interface IPSec)</b>	Applies a previously defined crypto map set to an interface.
<b>crypto map local-address</b>	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
<b>debug crypto isakmp</b>	Applies a previously defined crypto map set to an interface.
<b>match address (IPSec)</b>	Specifies an extended access list for a crypto map entry.
<b>set peer (IPSec)</b>	Specifies an IPSec peer in a crypto map entry.
<b>set pfs</b>	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
<b>set security-association level per-host</b>	Specifies that separate IPSec SAs should be requested for each source/destination host pair.
<b>set security-association lifetime</b>	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
<b>set session-key</b>	Specifies the IPSec session keys within a crypto map entry.
<b>set transform-set</b>	Specifies which transform sets can be used with the crypto map entry.
<b>show crypto map (IPSec)</b>	Displays the crypto map configuration.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

---

Copyright © 2002–2005 Cisco Systems, Inc. All rights reserved.

