



# L2TP—IPsec Support for NAT and PAT Windows Clients

---

The L2TP—IPsec Support for NAT and PAT Windows Clients feature allows more than one Windows client to connect to a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) at one time with IP Security (IPsec) enabled and a network address translation (NAT) or port address translation (PAT) server between the Windows client and LNS.

Currently, if one Windows client is connected to a Cisco IOS LNS router through a NAT or PAT server with IPsec enabled, and then another Windows client connects to the same Cisco IOS LNS router, the first client's connection is effectively terminated. Enabling L2TP—IPsec Support for NAT and PAT Windows Clients ensures that Windows client connections in this environment are established and maintained until the connection is closed.

## History for the L2TP—IPsec Support for NAT and PAT Windows Clients Feature

Release	Modification
12.3(11)T4	This feature was introduced.
12.4(1)	This feature was integrated into Release 12.4(1).

## 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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.

## Contents

- [Prerequisites for L2TP—IPsec Support for NAT and PAT Windows Clients, page 2](#)
- [Restrictions for L2TP—IPsec Support for NAT and PAT Windows Clients, page 2](#)
- [Information About L2TP—IPsec Support for NAT and PAT Windows Clients, page 2](#)
- [How to Enable L2TP—IPsec Support for NAT and PAT Windows Clients, page 4](#)
- [Configuration Examples for L2TP—IPsec Support for NAT and PAT Windows Clients, page 7](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 9](#)
- [Command Reference, page 11](#)

## Prerequisites for L2TP—IPsec Support for NAT and PAT Windows Clients

- You have an environment consisting of Windows clients and Cisco IOS LNS routers with IPsec enabled and a NAT or PAT server between the Windows client and LNS router.
- You must have a version of IPsec that contains the L2TP—IPsec Support for NAT and PAT Windows Clients feature.
- You must understand Windows 2000 concepts and configuration requirements.
- You must understand Cisco IOS LNS routers concepts and configuration requirements.
- You must understand NAT and PAT concepts and configuration requirements.
- You must understand IPsec concepts and configuration requirements.
- You must understand L2TP concepts and configuration requirements.

## Restrictions for L2TP—IPsec Support for NAT and PAT Windows Clients

- Tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.
- Port translation is not a standard default behavior. Port translation is incompatible with standard IPsec because it changes the LNS header port information.
- L2TP requires the client to have Microsoft DUN configured. L2TP is supported solely by Windows 2000 MS-DUN (L2TP is not supported by Windows 95, Windows 98, or Windows NT).

## Information About L2TP—IPsec Support for NAT and PAT Windows Clients

To use the L2TP—IPsec Support for NAT and PAT Windows Clients feature, the following concept should be understood:

- [How L2TP—IPsec Support for NAT and PAT Windows Clients Works, page 2](#)

## How L2TP—IPsec Support for NAT and PAT Windows Clients Works

With the L2TP—IPsec Support for NAT and PAT Windows Clients feature not enabled, Windows clients lose connection with the Cisco IOS LNS router when another Windows client establishes an IPsec-protected L2TP tunnel to the Cisco IOS LNS router when IPsec is enabled and there is a NAT or PAT server between the Windows clients and the LNS.

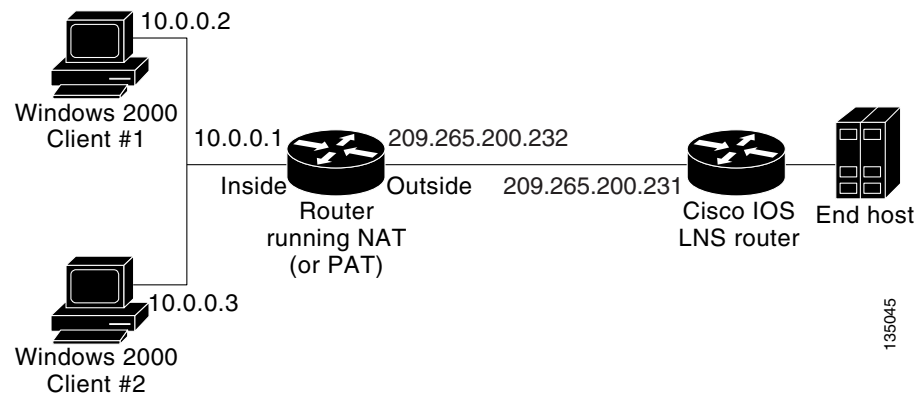
**Note**

If you do not have IPsec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

### Without L2TP—IPsec Support for NAT and PAT Windows Clients Feature Enabled

For example, [Figure 1](#) shows two Windows 2000 clients that are trying to connect to the end host through the router running NAT or PAT and the same Cisco IOS LNS router. IPsec is enabled.

**Figure 1** Multiple Windows 2000 Clients, NAT Router, and Cisco IOS LNS Router with IP Addresses



The Windows 2000 Client #1 establishes an IPsec-protected L2TP tunnel to the Cisco IOS LNS router. The Windows 2000 client and the Cisco IOS LNS router recognize that there is a router running NAT between them and IPsec and NAT-Traversal (NAT-T) are enabled. The Windows 2000 client attempts to establish an IPsec security association (SA) and requests transport mode (which it does by default) with proxies from 10.0.0.2, its local address, to 209.265.200.231, the Cisco IOS LNS router's address.

In transport mode NAT, running on the router, translates all outgoing connections (including 10.0.0.2) to its outside IP address (209.265.200.232), the address the traffic will come in on. However, NAT cannot modify the L2TP port designation (1701), which is protected by the IPsec encrypted area. So now, we have a local address of 209.265.200.231, a remote address of 209.265.200.232 and a remote port of 1701. All traffic is sent to the Windows 2000 Client #1 that matches the tunnel 209.265.200.231, port 1701.

Then Windows 2000 Client #2 establishes an IPsec-protected L2TP tunnel to the Cisco IOS LNS router, again in transport mode. And NAT, again, translates all outgoing connections to its outside IP address (209.265.200.232), but it cannot modify the L2TP port designation (1701). All traffic is now sent to Windows 2000 Client #2 that matches tunnel 209.265.200.231, port 1701. This second Windows client connection has effectively ended Windows Client #1's connection to the Cisco IOS LNS router since it is no longer receiving traffic.

### With L2TP—IPsec Support for NAT and PAT Windows Clients Feature Enabled

With the L2TP—IPsec Support for NAT and PAT Windows Clients feature enabled, IPsec can translate the L2TP ports after decryption. This feature allows IPsec to map traffic from different hosts to different source ports. L2TP can now distinguish between traffic destined for multiple Windows 2000 clients.

So now, when an SA is created, a translated port will be assigned to it. This port is client-specific. The same port will be used for any new SA created by that client. When an encrypted request is received and decrypted, the source port is translated from the standard value, 1701, to a client specific value. The request with the translated port is then forwarded to L2TP.

As shown in [Figure 1](#) with port translation enabled, the Windows 2000 Client #1 would have a translated port number of 1024 assigned and Windows 2000 Client #2 would have a translated port number of 1025 assigned.

When L2TP sends the reply packet, it uses the translated port number and creates a packet to that destination port. IPsec uses the destination port number to select the SA with which to encrypt the packet. Before encrypting the packet, IPsec translates the destination port back to the standard port number, 1701, which the Windows 2000 client expects. IPsec encrypts the packet, either with the SA to Windows 2000 Client #1 if the destination port was 1024 or with the SA to Windows 2000 Client #2 if the destination port was 1025. And now, all traffic is sent to the appropriate client and multiple Windows clients can be connected to a Cisco IOS LNS router through a NAT server at the same time.

The connection is maintained until one of the following actions occurs:

- The IPsec connection is closed.
- The NAT or PAT device ends the session.
- The LNS closes the session.
- The Windows client closes the session.

## How to Enable L2TP—IPsec Support for NAT and PAT Windows Clients

This section contains the following procedure that allows you to enable NAT/PAT port translation:

- [Enabling L2TP—IPsec Support, page 4](#)

### Enabling L2TP—IPsec Support

Use the following task to enable L2TP—IPsec Support for NAT and PAT Windows Clients for environments that have IPsec enabled and include multiple windows clients, a NAT or PAT server, L2TP, and a Cisco IOS LNS router.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]  
or  
**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
4. **set nat demux**
5. **exit**
6. **exit**
7. **show crypto map** [**interface** *interface* | **tag** *map-name*]  
or  
**show crypto dynamic-map** [**tag** *map-name*]
8. **show crypto ipsec sa**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>crypto map</b> <i>map-name</i> <i>seq-num</i> [<b>ipsec-isakmp</b>]</p> <p><b>Example:</b> Router(config)# crypto map STATIC_MAP 5</p> <p>or</p> <p><b>crypto dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-num</i></p> <p><b>Example:</b> Router(config)# crypto dynamic-map DYNAMIC_MAP 10</p>	<p>Names the static crypto map entry to create (or modify) and enters crypto map configuration mode.</p> <p>or</p> <p>Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode.</p>
Step 4	<p><b>set nat demux</b></p> <p><b>Example:</b> Router(config-crypto-map)# set nat demux</p>	<p>Enables L2TP—IPsec support.</p>
Step 5	<p><b>exit</b></p> <p><b>Example:</b> Router(config-crypto-map)# exit</p>	<p>Exits crypto map configuration mode and returns to global configuration mode.</p>
Step 6	<p><b>exit</b></p> <p><b>Example:</b> Router(config)# exit</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

	Command or Action	Purpose
Step 7	<pre>show crypto map [interface interface   tag map-name]</pre> <p><b>Example:</b> Router# show crypto map</p> <p>or</p> <pre>show crypto dynamic-map [tag map-name]</pre> <p><b>Example:</b> Router# show crypto dynamic-map</p>	<p>(Optional) Displays information about crypto map configuration.</p> <p>or</p> <p>(Optional) Displays information about dynamic crypto map configuration.</p>
Step 8	<pre>show crypto ipsec sa</pre> <p><b>Example:</b> Router# show crypto ipsec sa</p>	<p>(Optional) Displays the settings used by current SAs.</p>

## Configuration Examples for L2TP—IPsec Support for NAT and PAT Windows Clients

This section provides the following configuration example:

- [Dynamic Map Configuration: Example, page 7](#)

### Dynamic Map Configuration: Example

The following example shows how to enable the L2TP—IPsec Support for NAT and PAT Windows Clients feature for a dynamic crypto map:

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 72_LNS
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common
ip subnet-zero
!
!
no ip cef
no ip domain lookup
ip domain name cisco.com
```

```
ip dhcp excluded-address 20.0.0.8
ip dhcp excluded-address 20.0.0.10
!
!
ip vrf VPN
 rd 1:1
!
!Enable virtual private networking.
vpdn enable
vpdn ip udp ignore checksum
!
! Default L2TP VPDN group
vpdn-group L2TP
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
!protocol; specifies the number of the virtual templates used to clone
!virtual-access interfaces
 accept-dialin
  protocol l2tp
  virtual-template 1

!Disables L2TP tunnel authentication.
no l2tp tunnel authentication
!
!
crypto keyring L2TP
 pre-shared-key address 0.0.0.0 0.0.0.0 key *****
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
!
crypto isakmp key cisco hostname w2k01
crypto isakmp keepalive 3600
!
crypto ipsec security-association lifetime seconds 600
!
!Defines a transform set.
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
 mode transport
!
!Names the dynamic crypto map entry and enters crypto map configuration mode; Enables
!L2TP—IPSec support; Specifies which transform sets can be used with the crypto map
!entry
crypto dynamic-map DYN_MAP 10
 set nat demux
 set transform-set TS1!
!
crypto map CRYP_MAP 6000 ipsec-isakmp dynamic DYN_MAP
!
interface Loopback0
 ip address 12.0.0.8 255.255.255.255
!
interface FastEthernet0/0
 ip address 11.0.0.8 255.255.255.0
 no ip route-cache
 duplex full
 speed 100
 crypto map CRYP_MAP
!
interface FastEthernet0/1
```

```

ip address 20.0.0.8 255.255.255.0
duplex full
speed 100
!
interface FastEthernet2/0
ip address 172.19.192.138 255.255.255.0
duplex full
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool POOL
ppp mtu adaptive
ppp authentication chap ms-chap
!
router ospf 1
log-adjacency-changes
redistribute static subnets
network 11.0.0.0 0.0.0.255 area 0
!
ip local pool POOL 20.0.0.100 20.0.0.110
ip classless
ip route 171.0.0.0 255.0.0.0 172.19.192.1
!
no ip http server
no ip http secure-server
!
!
control-plane
!
gatekeeper
shutdown!
!
line con 0
exec-timeout 0 0
logging synchronous
stopbits 1
line aux 0
stopbits 1
line vty 0 4
!
end

```

## Additional References

The following sections provide references related to L2TP—IPsec Support for NAT and PAT Windows Clients.

## Related Documents

Related Topic	Document Title
IP security and encryption	<a href="#">Security for VPNs with IPsec</a>

## Standards

Standard	Title
None	—

## MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
None	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*.

- **set nat demux**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Master Command List*.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009–2010 Cisco Systems, Inc. All rights reserved.

