Chapter 13

Securing L2TP and IP Tunnels with IPSec

This chapter describes how to secure generic routing encapsulation (GRE), Distance Vector Multicast Routing Protocol (DVMRP), and Layer 2 Tunneling Protocol (L2TP) tunnels with IP Security (IPSec) on your E-series router. It contains the following sections:

Overview

You can provide additional security to L2TP and IP tunnels by protecting them with an IPSec transport connection. Secure IP interfaces are virtual IP interfaces that are configured to provide confidentiality and authentication services for the traffic flowing through the interface; that traffic can be L2TP, GRE, and DVMRP tunnel traffic. See *Chapter 6, Configuring IPSec* for detailed information about IPSec.

GRE, DVMRP, and L2TP over IPSec provide security only between tunnel endpoints; they do not provide end-to-end security. For end-to-end security, you need additional security for the connection beyond the router.

Tunnel Creation

ERX routers can have both unsecured GRE, DVMRP, and L2TP tunnels and tunnels that are secured by IPSec. However, unsecured L2TP tunnels are not allowed on the ISM. You use the following commands to create a secure tunnel:

- L2TP tunnels—Use the **enable ipsec transport** command in the L2TP destination profile
- GRE and DVMRP tunnels—Use the **ipsec-transport** keyword in the **interface tunnel** command

IPSec Secured-Tunnel Maximums

See *JUNOSe Release Notes, Appendix A, System Maximums* corresponding to your software release for information about the maximum number of GRE/IPSec, DVMRP/IPSec, and L2TP/IPSec connections supported on E-series routers.

Platform Considerations

For information about modules that support L2TP and IP tunnels with IPSec on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See LNS and LAC support in *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See LNS and LAC support in *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support LNS and LAC.

For information about modules that support L2TP and IP tunnels with IPSec on the E120 router and the E320 router:

- See LNS and LAC support in *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See LNS and LAC support in *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support LNS and LAC.

Module Requirements

To create IPSec-secured tunnels, you must install an IPSec Service module (ISM) in the ERX router. The ISM is a security gateway and functions as one of the endpoints for secure tunnels. The tunnel endpoints are the tunnel *source* and the tunnel *destination* IP addresses. For an L2TP/IPSec tunnel, the source is the L2TP network server (LNS) and the destination is the L2TP access concentrator (LAC).

For information about installing ISMs in the ERX routers, see the *ERX Hardware Guide*.

References

For more information about the protocols for securing L2TP and IP tunnels with IPSec, consult the following resources:

- RFC 2401—Security Architecture for the Internet Protocol (November 1998)
- RFC 2661—Layer Two Tunneling Protocol "L2TP" (August 1999)
- RFC 3193—Securing L2TP using IPSec (November 2001)
- RFC 3715—IPsec-Network Address Transation (NAT) Compatibility Requirements (March 2004)
- Negotiation of NAT-Traversal in the IKE—draft-ietf-ipsec-nat-t-ike-08.txt (July 2004 expiration)
- UDP Encapsulation of IPsec ESP Packets—draft-ietf-ipsec-udp-encaps-09.txt (November 2004 expiration)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

For additional configuration information, see:

- *Chapter 6, Configuring IPSec*
- *Chapter 9, Configuring Digital Certificates*
- *Chapter 10, Configuring IP Tunnels*
- *JUNOSe Broadband Access Configuration Guide, Chapter 10, L2TP Overview*

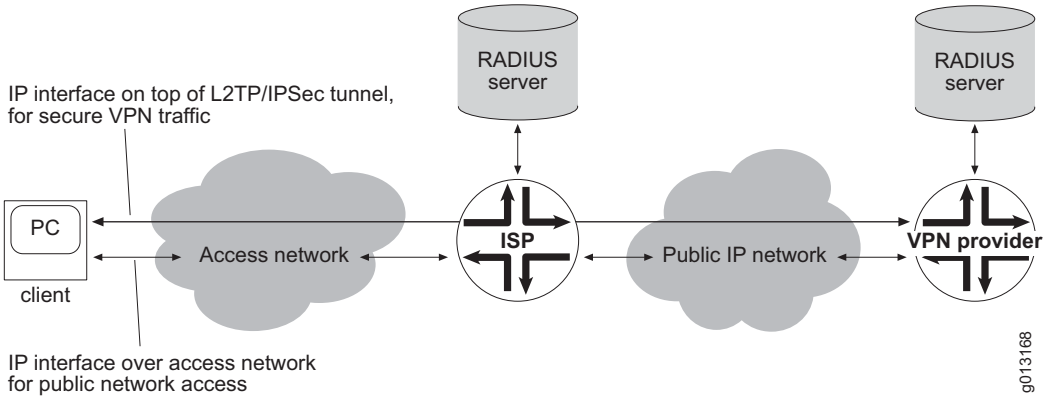
L2TP/IPSec Tunnels

L2TP/IPSec remote access allows clients to connect to a corporate VPN over the public Internet with a secure connection. The L2TP tunnel runs on top of an IPSec transport mode connection. The secure tunnel runs from the client PC to the E-series router that terminates the secure tunnel. For example, using L2TP with IPSec enables B-RAS clients to securely connect to a corporate or other VPN in addition to using another unsecured connection to the Internet, depending on the client software capabilities.

On the router side of the L2TP connection, the E-series router acts as the LNS. On the PC client side of the connection, the client acts as the LAC and runs the L2TP/IPSec client software on supported platforms. (For a list of the supported platforms, see *Client Software Supported* on page 308.) Both sides of the connection run IPSec in transport mode with Encapsulating Security Payload (ESP) encryption and authentication.

In the model shown in Figure 22 on page 306, a client PC connects to its local provider, who gives the client a public IP address. Using the public IP address, the client PC initiates an IPSec connection toward the L2TP/IPSec gateway for the private network that it wants to connect to. After establishing the IPSec connection, the client establishes an L2TP tunnel to the same L2TP/IPSec gateway, which provides the client with another IP interface to access the private network it is connecting to. The L2TP tunnel is completely protected by the IPSec connection established earlier.

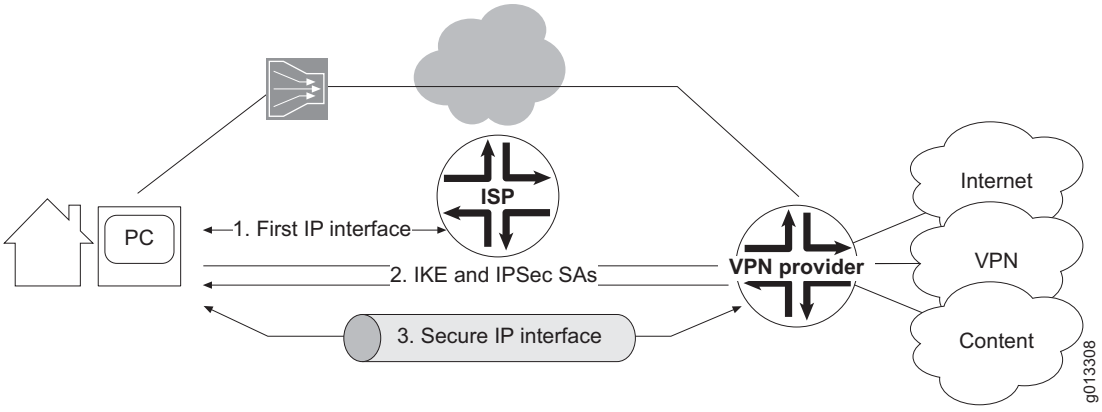
Figure 22: L2TP with IPSec Application



Setting Up the Secure L2TP Connection

Figure 23 gives an overview of the process used to set up a secure connection between the client PC and an E-series router that is acting as a VPN provider.

Figure 23: L2TP/IPSec Connection



To set up the secure connection shown in Figure 23:

1. Obtain an IP address from your ISP, using a normal B-RAS termination.
2. IKE signals a security association (SA) between the client PC and the E-series router that is acting as a VPN provider.
   - SAs are established to secure data traffic.
   - The IPSec connection secures L2TP traffic.
3. Set up an L2TP tunnel and session between the client PC (the LAC) and the E-series router (the LNS).

   The tunnel runs over the SAs that IKE established.

L2TP with IPSec Control and Data Frames

L2TP and IPSec define control and data messages used for L2TP/IPSec. Figure 24 shows an L2TP control frame encapsulated by IPSec. The shaded area shows the encrypted portion of the frame.

Figure 24: L2TP Control Frame Encapsulated by IPSec

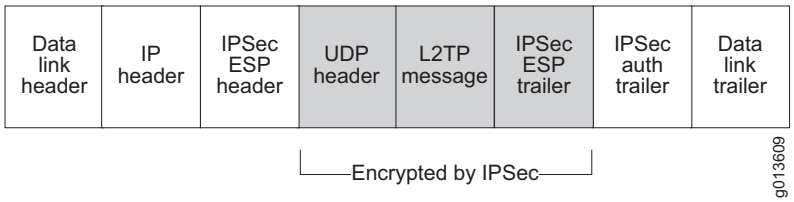
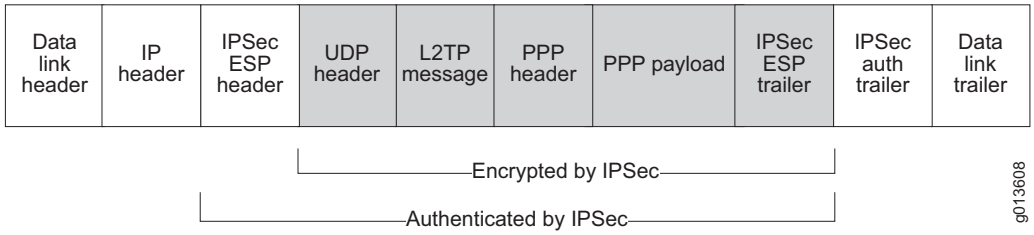


Figure 25 is an L2TP data frame encapsulated by IPSec. The shaded area shows the encrypted portion of the frame.

Figure 25: L2TP Data Frame Encapsulated by IPSec



Compatibility and Requirements

This section covers various compatibility issues and requirements for the L2TP/IPSec traffic.

Client Software Supported

The L2TP/IPSec software supports the following client PC operating systems and L2TP and IPSec applications:

- Windows 2000 and Windows XP running built-in IPSec VPN software
- Microsoft L2TP/IPSec VPN client for Windows NT, Windows 98, and Windows Me
- SafeNet client software
- Mac OS X version 10.3 or higher

Interactions with NAT

There are two ways that you can configure E-series routers to interact with Network Address Translation (NAT) devices in the network:

- Configure the router to run in NAT passthrough mode by using the **application l2tp-nat-passthrough** command. For information, see *NAT Passthrough Mode* on page 309.
- Configure the virtual router to enable NAT Traversal (NAT-T) by using the **ipsec option nat-t** command. For information, see *NAT Traversal* on page 309.

Interaction Between IPSec and PPP

PPP defines the Compression Control Protocol (CCP) and the Encryption Control Protocol (ECP) modes. These modes are currently not supported in the E-series router. There is no interaction related to encryption directives between IPSec and PPP.

LNS Change of Port

In the L2TP world, the LNS is allowed to change its port number; this functionality is currently not supported in ERX routers. IPSec allows only port 1701 to be used for L2TP/IPSec tunnels. However, the LAC is allowed to use any source port it desires.

Group Preshared Key

Group preshared keys allow the provisioning of secure remote access by means of L2TP/IPSec to networks that do not use a certificate authority (CA) to issue certificates. A group preshared key is associated with a local IP address in the E-series router and is used to authenticate L2TP/IPSec clients that target this IP address as their VPN server address.

CAUTION: Group preshared keys are not fully secure, and we recommend that you use digital certificates in place of group preshared keys. Group preshared keys are open to man-in-the-middle attacks. To reduce this risk, the ERX routers accept only IPSec connections that specify L2TP traffic selectors for security associations (SAs) that are negotiated over IKE connections authenticated with group preshared keys.

NAT Passthrough Mode

NAT devices can change the IP address and port number of a traversing IP packet. Encrypted frames, in which an ESP header follows the IP header, may or may not get through the NAT device.

You can set up the router to run in NAT passthrough mode, which causes the router to not check UDP checksums. The reason is that a NAT device may change the IP address while the UDP header is encrypted. In this case, the UDP checksum cannot be recalculated. Not checking UDP checksums does not compromise security, because IPSec protects UDP with an authentication algorithm far stronger than UDP checksums. To set up the router to run in NAT passthrough mode, use the **application l2tp-nat-passthrough** command.

We recommend that you configure the router to use NAT passthrough mode when the NAT device provides a feature commonly known as IPSec passthrough.

For information about configuring NAT passthrough mode as part of an IPSec transport profile, see *Configuring IPSec Transport Profiles* on page 319.

NAT Traversal

Using NAT passthrough mode is an adequate solution when a single remote user located behind a NAT device needs secure access to an E-series router. However, NAT passthrough mode does not support secure access to the router by multiple remote users at locations such as hotels or airports where a NAT device resides between the router and the remote users. In addition, NAT passthrough mode does not provide secure access for groups of remote users at corporate locations where a NAT device resides between the company's intranet and the public IP network.

To allow secure router access for multiple remote hosts located behind a NAT device, the router supports a set of IETF standards collectively known as NAT Traversal (NAT-T). For a list of the individual standards that NAT-T comprises, see *References* on page 305.

How NAT-T Works

By default, NAT-T is enabled on every virtual router configured on the system. With NAT-T enabled, IPSec traffic flows transparently through a NAT device, thereby allowing one or more remote hosts located behind the NAT device to use secure L2TP/IPSec tunnel connections to access the router.

After NAT-T is enabled on a specific virtual router, either by default or by using the **ipsec option nat-t** command, the router performs the following actions, in this order:

1. The router monitors the exchange of private vendor ID (VID) payloads between the client PC and the E-series router during the IKE SA negotiation to determine whether both sides of the negotiation support NAT-T.

2. If both sides of the negotiation support NAT-T, the router detects whether a NAT device resides between the IPSec remote peers.

3. If a NAT device is detected between the remote peers, the router negotiates the appropriate type of UDP encapsulation as part of the IKE SA and uses this encapsulation method to process the IPSec traffic.

The **ipsec option nat-t** command affects only those IKE SAs negotiated on the virtual router *after* the command is issued. The command has no effect on IKE SAs that were previously negotiated.

UDP Encapsulation

As part of the IKE SA negotiation process, the router automatically negotiates UDP encapsulation for L2TP/IPSec control and data frames.

When NAT-T is enabled, L2TP/IPSec control frames and data frames are wrapped in an additional NAT-T UDP header that enables data to flow transparently through the NAT device. The NAT device can translate the IP address of the source port associated with the NAT-T UDP header, whereas the IPSec ESP header does not have a source port that the NAT device can translate.

Figure 26 shows an L2TP control frame encapsulated with a NAT-T UDP header. The shaded area shows the portion of the frame that is encrypted by IPSec.

Figure 26: L2TP Control Frame with NAT-T UDP Encapsulation

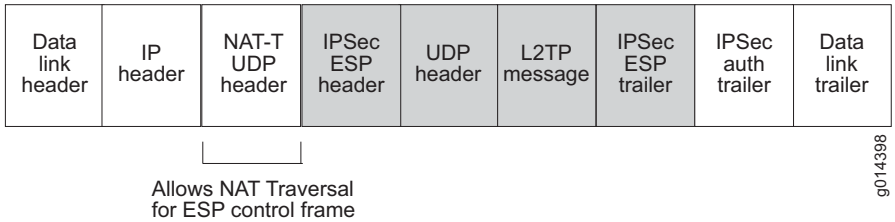
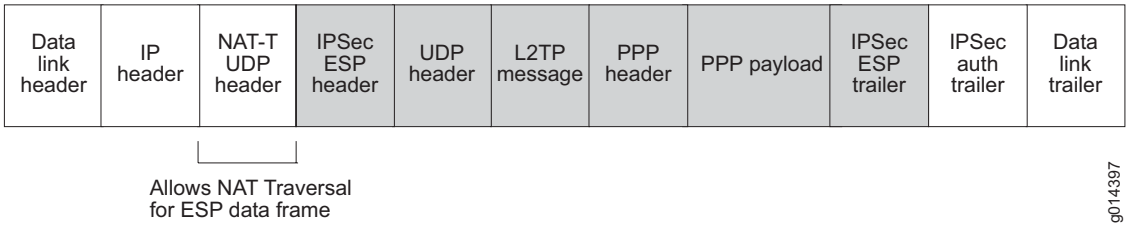


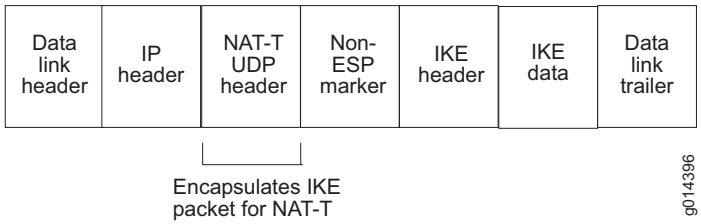
Figure 27 shows an L2TP data frame encapsulated with a NAT-T UDP header. The shaded area shows the portion of the frame that is encrypted by IPSec.

Figure 27: L2TP Data Frame with NAT-T UDP Encapsulation



Additionally, IKE packets transmitted during the IKE SA negotiation process are encapsulated with a NAT-T UDP header, and include a non-ESP marker to distinguish them from standard ESP control and data frames. Figure 28 shows an IKE packet encapsulated with a NAT-T UDP header.

Figure 28: IKE Packet with NAT-T UDP Encapsulation



Only frames that use the ESP encryption and authentication protocol can be UDP-encapsulated. Frames that use authentication header (AH) cannot be UDP-encapsulated; therefore, NAT-T is *not supported* for L2TP/IPSec connections that use AH.

For more detailed information about encapsulation and other IPSec security parameters, see *Chapter 6, Configuring IPSec*.

UDP Statistics

When NAT-T is enabled, UDP-encapsulated IPSec packets arriving and leaving the router look like standard UDP packets. However, the router does not forward these packets to and from the SRP module, as it does for other UDP packets. As a result, the UDP statistics maintained by the SRP module do not reflect UDP-encapsulated IPSec packets.

NAT Keepalive Messages

The router does not generate NAT keepalive messages. The following reasons explain why this behavior does not generally pose problems for remote users.

- The primary application for using NAT-T is enabling secure L2TP/IPSec access to an E-series router for remote hosts located behind a NAT device. The L2TP protocol has its own keepalive mechanism that is sufficient for keeping NAT entries alive.
- In most NAT configurations, an ERX router does not operate behind the NAT device, thereby making the generation of keepalive messages unnecessary.

If the router receives NAT keepalive messages as part of the L2TP/IPSec traffic flow, it discards these messages at the ingress line module on which the messages were received.

Configuring and Monitoring NAT-T

For instructions on configuring and monitoring NAT-T, see the sections listed in Table 18.

Table 18: Configuration and Monitoring Tasks for NAT-T

Task	Command	See Section
Enabling and disabling NAT-T on a virtual router	**ipsec option nat-t**	*Configuring NAT-T* on page 315
Displaying information about the current NAT-T setting on a virtual router	**show ipsec option**	*Monitoring DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec Tunnels* on page 325
Displaying information about the IKE SA negotiation when NAT-T is enabled	**show ipsec ike-sa**	*Monitoring DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec Tunnels* on page 325

Single-Shot Tunnels

You can use the **single-shot-tunnel** command in L2TP Destination Profile Host Configuration mode to configure a single-shot L2TP tunnel. Although configuration of single-shot tunnels is more typically used with secure L2TP/IPSec tunnels, as described in this chapter, you can also configure single-shot tunnels for nonsecure L2TP tunnels that do not run over an IPSec connection.

A *single-shot tunnel* has the following characteristics:

- The L2TP tunnel can carry no more than a single L2TP session for the duration of its existence.
- The router ignores the idle timeout period for single-shot tunnels. This means that as soon a single-shot tunnel's session is removed, the single-shot tunnel proceeds to disconnect.
- The following characteristics apply only to secure L2TP/IPSec single-shot tunnels:
  - The underlying IPSec connection for a single-shot tunnel can carry no more than a single L2TP tunnel for the duration of its existence.
  - The router disconnects the underlying IPSec transport connection for a single-shot tunnel at the beginning of the destruct timeout period instead of waiting until the destruct timeout period expires.

For L2TP/IPSec single-shot tunnels, as soon as the tunnel or its single session fails negotiations or disconnects, the router prevents any further L2TP tunnels or L2TP sessions from connecting, and requires that a new IPSec connection be established for any subsequent connection attempts.

Table 19 describes the differences between how the router handles the idle timeout period (configured with the **l2tp tunnel idle-timeout** command) and the destruct timeout period (configured with the **l2tp destruct-timeout** command) for standard L2TP/IPSec tunnels and for single-shot L2TP/IPSec tunnels when the last remaining tunnel session has been disconnected.

Table 19: Differences in Handling Timeout Periods for L2TP/IPSec Tunnels

Timeout Period	Standard L2TP/IPSec Tunnels (Not Single-Shot)	Single-Shot L2TP/IPSec Tunnels
Idle timeout period	The tunnel persists until the idle timeout period expires. If a new L2TP session is created before the idle timeout period expires, the tunnel persists to carry the new session and any subsequent sessions that are established. When the idle timeout period expires, the router disconnects the tunnel.	The router ignores the idle timeout period. This behavior prevents a single-shot tunnel from passing traffic after its single L2TP session is disconnected.
Destruct timeout period	The router signals the underlying IPSec transport connection to disconnect when the destruct timeout period expires.	The router signals the underlying IPSec transport connection to disconnect at the beginning of the destruct timeout period.

For information about configuring L2TP/IPSec single-shot tunnels on the router, see *Configuring Single-Shot Tunnels* on page 316.

Configuration Tasks for Client PC

To set up client PCs, you need to:

1. Create an IPSec security policy to secure L2TP traffic to the E-series router.
2. Get a certificate for the client or set up preshared keys.
3. Create a VPN connection to the router.
4. Log the client in to the E-series router.

Configuration Tasks for E-series Routers

The main configuration tasks for setting up L2TP/IPSec are:

1. Set up IP connectivity to L2TP clients; for example, PPPoE, DHCP, or static IP.
2. Set up digital certificates on the router, or configure preshared keys for IKE authentication.
   - To set up digital certificates, see *Chapter 9, Configuring Digital Certificates*.
   - To set up preshared keys, see *Configuring IPSec Parameters* in *Chapter 6, Configuring IPSec*.
3. Create IPSec policies. See *Defining an IKE Policy* in *Chapter 6, Configuring IPSec*.
4. Configure RADIUS authentication and accounting. See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*.

5. Configure L2TP destination profiles. See the next section, *Enabling IPSec Support for L2TP*.

6. Configure NAT-T on the virtual router. See *Configuring NAT-T* on page 315.

7. Configure single-shot L2TP/IPSec tunnels. See *Configuring Single-Shot Tunnels* on page 316.

8. Configure IPSec transport profiles. See *Configuring IPSec Transport Profiles* on page 319.

Enabling IPSec Support for L2TP

To configure an L2TP destination profile:

1. Create a destination profile that defines the location of the LAC, and access L2TP Destination Profile Configuration mode.

   ```
   host1(config)#l2tp destination profile boston4 ip address 0.0.0.0
   host1(config-l2tp-dest-profile)#
   ```

2. Define the L2TP host profile, and enter L2TP Destination Profile Host Configuration mode.

   ```
   host1(config-l2tp-dest-profile)#remote host default
   host1(config-l2tp-dest-profile-host)#
   ```

3. Specify that for L2TP tunnels associated with this destination profile, the router accept only tunnels protected by IPSec.

   ```
   host1(config-l2tp-dest-profile-host)#enable ipsec-transport
   ```

4. (Optional) Assign a profile name for a remote host.

   ```
   host1(config-l2tp-dest-profile-host)#profile georgeProfile1
   ```

5. Specify the local IP address to be used in any packets sent to the LAC.

   ```
   host1(config-l2tp-dest-profile-host)#local ip address 10.0.0.1
   ```

For information about other L2TP destination profile commands, see *JUNOSe Broadband Access Configuration Guide, Chapter 12, Configuring an L2TP LNS*.

enable ipsec-transport

- Use to specify that the router accept only L2TP tunnels protected by an IPSec transport connection.
- Example

  ```
  host1(config-l2tp-dest-profile-host)#enable ipsec-transport
  ```

- Use the **no** version to disable IPSec transport mode.

l2tp destination profile

- Use to create the destination profile that defines the location of the LAC and to access L2TP Destination Profile Configuration mode.
- If no virtual router is specified, the current virtual router context is used.
- If the destination address is 0.0.0.0, then any LAC that can be reached via the specified virtual router is allowed to access the LNS. If the destination address is nonzero, then it must be a host-specific IP address.
- The router supports up to 4,000 L2TP destination profiles.
- Example

  host1:boston(config)#**l2tp destination profile boston ip address 10.10.76.12**
  host1:boston(config-l2tp-dest-profile)#

- Use the **no** version to remove the L2TP destination profile and all of its host profiles.

NOTE: If you remove a destination profile, all tunnels and sessions using that profile will be dropped.

Configuring NAT-T

To configure NAT-T on the current virtual router:

1. Select the name of the virtual router you want to configure.

   host1(config)#**virtual-router westford**
   host1:westford(config)#

2. Enable NAT-T for the current virtual router.

   host1:westford(config)#**ipsec option nat-t**

ipsec option nat-t

- Use to enable NAT-T for the current virtual router.
- With NAT-T enabled, IPSec traffic flows transparently through a NAT device, thereby allowing one or more remote hosts located behind the NAT device to use secure L2TP/IPSec tunnel connections to access the router.
- The **ipsec option nat-t** command affects only those IKE SAs negotiated on this virtual router after the command is issued; it has no effect on previously negotiated IKE SAs.
- Example

  host1:sunnyvale(config)#**ipsec option nat-t**

- Use the **no** version to disable NAT-T for the current virtual router.
- Use the **default** version to restore the default NAT-T setting on the virtual router, enabled.

Configuring Single-Shot Tunnels

To configure a single-shot L2TP/IPSec tunnel:

1. Create an L2TP destination profile, which defines the location of the LAC. The **l2tp destination profile** command accesses L2TP Destination Profile Configuration mode.

   host1(config)#**l2tp destination profile boston4 ip address 0.0.0.0**
   host1(config-l2tp-dest-profile)#

2. Create an L2TP host profile, which defines the attributes that the router, acting as the LNS, uses when communicating with the LAC. The **remote host** command accesses L2TP Destination Profile Host Configuration mode.

   host1(config-l2tp-dest-profile)#**remote host default**
   host1(config-l2tp-dest-profile-host)#

3. Specify that, for L2TP tunnels associated with this host profile, the router accept only tunnels protected by IPSec.

   host1(config-l2tp-dest-profile-host)#**enable ipsec-transport**

4. Specify that the L2TP tunnels associated with this host profile are single-shot tunnels.

   host1(config-l2tp-dest-profile-host)#**single-shot-tunnel**

5. (Optional) Configure other attributes for the L2TP host profile.

6. (Optional) Use the **show l2tp destination profile** command to verify configuration of the single-shot tunnel for a particular L2TP host profile.

   For information about how to use this command, see **show l2tp destination profile** on page 330.

For information about the other commands you can use to configure L2TP destination profiles and L2TP host profiles, see *JUNOSe Broadband Access Configuration Guide, Chapter 12, Configuring an L2TP LNS*.

single-shot-tunnel

- Use to configure the L2TP/IPSec tunnels associated with a particular L2TP host profile as single-shot tunnels.
- A single-shot tunnel can carry no more than a single L2TP session for the duration of its existence.
- The router ignores the idle timeout period for single-shot tunnels.

- The following characteristics apply only to secure L2TP/IPSec single-shot tunnels:
  - The underlying IPSec connection for a single-shot tunnel can carry no more than a single L2TP tunnel for the duration of its existence.
  - The router disconnects the underlying IPSec transport connection for a single-shot tunnel at the beginning of the destruct timeout period instead of waiting until the destruct timeout period expires.
- A single-shot tunnel does not persist beyond its last connected L2TP session. As a result, using single-shot L2TP/IPSec tunnels instead of the default (standard) tunnel behavior provides better protection against a brute force attack that makes multiple, simultaneous authentication attempts.
- Example

  host1(config-l2tp-dest-profile-host)#**single-shot-tunnel**

- Use the **no** version to restore the default behavior for L2TP/IPSec tunnels, which disables the single-shot attribute.

GRE/IPSec and DVMRP/IPSec Tunnels

In GRE/IPSec or DVMRP/IPSec connections, E-series routers can act as source and destination endpoints of the secure tunnel. Both sides of the connection run IPSec in transport mode with Encapsulating Security Payload (ESP) encryption and authentication.

In a GRE/IPSec or DVMRP/IPSec connection, the E-series router initiates an IPSec connection with a remote router. After establishing the IPSec connection, the E-series router establishes a GRE or DVMRP tunnel to the remote router. The tunnel is completely protected by the IPSec connection.

Setting Up the Secure GRE or DVMRP Connection

In Figure 29, a secure GRE/IPSec connection is set up between two E-series routers. To set up the secure connection:

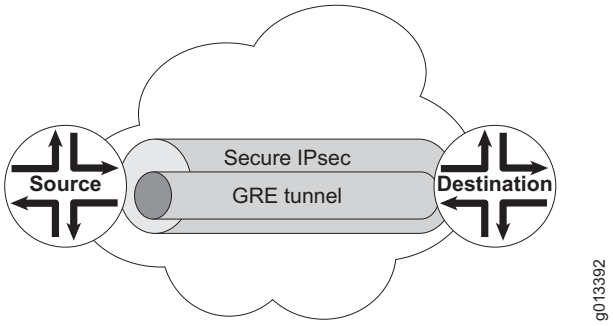
1. Set up the IPSec connection between the two routers. IKE signals a security association (SA) between the two IPSec tunnel endpoints.

   Two unidirectional SAs are established to secure data traffic.

2. Set up a GRE tunnel between the two routers.

The GRE tunnel now runs over the SAs that IKE established.

Figure 29: GRE/IPSec Connection



Configuration Tasks

The main configuration tasks for setting up GRE or DVMRP over IPSec on E-series routers are:

- Set up the GRE or DVMRP tunnel, specifying the virtual router and destination address, and enabling IPSec support. See *Chapter 10, Configuring IP Tunnels*.
- Set up digital certificates on the router, or configure preshared keys for IKE authentication.
  - To set up digital certificates, see *Chapter 9, Configuring Digital Certificates*.
  - To set up preshared keys, see *Configuring IPSec Parameters* in *Chapter 6, Configuring IPSec*.
- Create IPSec policies. See *Defining an IKE Policy* in *Chapter 6, Configuring IPSec*.
- Configure IPSec transport profiles. See *Configuring IPSec Transport Profiles* on page 319.

Enabling IPSec Support for GRE and DVMRP Tunnels

To create GRE/IPSec and DVMRP/IPSec tunnels, use the **ipsec-transport** keyword with the **interface tunnel** command.

interface tunnel dvmrp
interface tunnel gre

- Use with the **ipsec-transport** keyword to create a GRE or DVMRP tunnel that is protected with IPSec in transport mode.

NOTE: After you create a clear GRE or DVMRP tunnel, you cannot convert it to an IPSec-secured tunnel, or vice versa. You must delete the tunnel configuration, then reconfigure the tunnel as the new type.

- You can establish the tunnel on a virtual router other than the current virtual router.
- Example

  host1(config)#**interface tunnel gre:denver-tunnel-5 transport-virtual-router denver ipsec-transport**
  host1(config-if)#

- Use the **no** version to remove the tunnel.

Configuring IPSec Transport Profiles

To configure an IPSec transport profile that will be used to secure DVMRP, GRE, or L2TP tunnels:

1. Create the profile.

   host1(config)#**ipsec transport profile secureGre virtual-router default ip address 5.5.5.5**
   host1(config-ipsec-transport-profile)#

2. Specify one or more types of application that the profile secures.

   host1(config-ipsec-transport-profile)#**application gre dvmrp l2tp**

You can then set any of the following parameters for the profile:

- Set a lifetime range for the IPSec connection in volume of traffic or seconds.

  host1(config-ipsec-transport-profile)#**lifetime seconds 3600 28800 kilobytes 102400 4294967295**

- Configure Perfect Forward Secrecy (PFS) for connections created with this IPSec transport profile.

  host1(config-ipsec-transport-profile)#**pfs group 5**

- Specify one or more transform sets that an IPSec transport connection uses to negotiate a transform algorithm.

  host1(config-ipsec-transport-profile)#**transform-set esp-3des-hmac-sha esp-3des-hmac-md5**

  To display the available transform sets, issue the **transform-set ?** command.

- Specify the local endpoint (for L2TP, the LNS address) of the IPSec transport connection, and enter Local IPSec Transport Profile mode.

  host1(config-ipsec-transport-profile)#**local ip address 10.10.1.1**
  host1(config-ipsec-transport-profile-local)#

- (Optional) Configure a key for IKE negotiations. For example:

  Enter the unencrypted key. The router encrypts the key and stores it in encrypted form. You can no longer retrieve the unencrypted key.

  host1(config-ipsec-transport-profile-local)#**pre-share secretforGre**

application

- Use to specify the types of application secured by connections created with this IPSec transport profile. You can specify multiple applications on the same command line:
  - **dvmrp**—Secures DVMRP tunnel traffic
  - **gre**—Secures GRE tunnel traffic
  - **l2tp**—Secures L2TP traffic
  - **l2tp-nat-passthrough—**Secures L2TP traffic and also allows clients to connect from behind NAT devices that support IPSec passthrough. To allow these clients to connect, the router:
    - Does not generate or verify UDP checksums. This does not compromise security, because IPSec protects UDP packets with an authentication algorithm far stronger than UDP checksums.
    - Provides IPSec filtering based on the received IP address (the NAT public IP address), rather than filtering based on the negotiated IKE identities.
- Example

  host1(config-ipsec-transport-profile)#**application gre dvmrp l2tp**

- Use the **no** version to return to the default application type, L2TP.

ipsec transport profile

- Use to create an IPSec transport profile and to enter IPSec Transport Profile Configuration mode. To create a new profile, you must include the following keywords:
  - **virtual-router—**Name of the virtual router on which you want to create the profile
  - **ip address**—Remote endpoint for the IPSec transport connection.

    For L2TP/IPSec connections, you can enter a fixed IP address or the wildcard address, 0.0.0.0. If you use the wildcard address, the profile accepts any remote client connection, which is a typical scenario for secure remote access.

    For GRE/IPSec and DVMRP/IPSec connections, you must enter a fixed address; the 0.0.0.0 wildcard address is not accepted and will return an error.
- Example

  host1(config)#**ipsec transport profile secureL2tp virtual-router default ip address 5.5.5.5**
  host1(config-ipsec-transport-profile)#
- Use the **no** version to delete the profile.

lifetime

- Use to set a lifetime range for the IPSec connection in volume of traffic or in seconds or both.
- If the PC client offers a lifetime within this range, the router accepts the offer. If the PC client offers a lifetime outside this range, the router rejects the connection.
- Example

  host1(config-ipsec-transport-profile)#**lifetime seconds 900 86400 kilobytes 100000 4294967295**
- Use the **no** version to restore the default values, 100000–4294967295 KB and 900–86400 seconds (0.25–24 hours).

local ip address

- Use to specify the local endpoint (for L2TP, the LNS address) of the IPSec transport connection and to enter Local IPSec Transport Profile Configuration mode.
- You can enter this command multiple times in an IPSec transport profile.
- You can enter a fixed IP address or the wildcard address, 0.0.0.0. The wildcard address has a lower precedence than a fixed IP address.

CAUTION: We recommend that you do not use address 0.0.0.0, because it allows any address to accept IKE calls, and it creates a group preshared key, which is not fully secure.

- Example

  host1(config-ipsec-transport-profile)#**local ip address 192.168.1.2**
  host1(config-ipsec-transport-profile-local)#

- Use the **no** version to delete the IP address.

pfs group

- Use to configure perfect forward secrecy for connections created with this IPSec transport profile.
- Assign a Diffie-Hellman prime modulus group using one of the following keywords:
  - **1**—768-bit group
  - **2**—1024-bit group
  - **5**—1536-bit group
- Example

  host1(config-ipsec-transport-profile)#**pfs group 5**

- Use the **no** version to remove PFS from this profile, which is the default setting.

pre-share

- Use to configure an unencrypted (red) preshared key to authenticate IKE negotiations that arrive from any remote IP address specified for this transport profile and that are destined for the local IP address. If the remote endpoint address is a wildcard address, this preshared key is a group preshared key.

CAUTION: Group preshared keys are not fully secure, and we do not recommend using them. They are provided for trials and testing purposes where the missed security does not pose a risk to the provider.

- To have preshared key authentication take place, you must also specify the IKE policy rule as preshared by entering **authentication pre-share** in ISAKMP Policy Configuration mode.
- Example

  host1(config-ipsec-transport-profile-local)#**pre-share secretforL2tp**

- Use the **no** version to remove the key.

NOTE: After you enter a preshared key, the original (unencrypted) key cannot be retrieved. If you need to reenter the original key (for example, the system goes to factory default and you have only the **show config** output) you can:

1. Use the **show config** command to see the encrypted (masked) form of the key.
2. Use the **pre-shared-masked** command to enter the masked key. The system will behave the same as when you entered the first **pre-share** key command.

pre-share-masked

- Use to specify an encrypted preshared key. To obtain this key, you enter an unencrypted key using the **pre-share** command. You then run the **show config** command, and the router displays the preshared key in encrypted form. You enter the encrypted key using the **pre-share-masked** command.
- The router uses the preshared key to authenticate IKE negotiations that arrive from any remote IP address specified for this transport profile and that are destined for any local IP address specified for this transport profile. If the remote endpoint address is a wildcard address, this preshared key is a group preshared key.

CAUTION: Group preshared keys are not fully secure, and we do not recommend using them. They are provided for trials and testing purposes, where the missed security does not pose a risk to the provider.

- To have preshared key authentication take place, you must also specify the IKE policy rule as preshared by entering **authentication pre-share** in ISAKMP Policy Configuration mode.
- Example

  host1(config-ipsec-transport-profile-local)#**pre-share-masked AAAAGAAAAAcAAAACZquq4ABieTUBuNBELSY8b/L3CX/RcPX7**

- There is no **no** version. To remove a key, use the **no pre-share** command.

transform-set

- Use to specify the transform set(s) that an IPSec transport connection can use to negotiate a transform algorithm. Each transform in the set provides a different combination of data authentication and confidentiality.
- To display the available transform sets, issue the **transform-set ?** command.
- Example

  host1(config-ipsec-transport-profile)#**transform-set esp-3des-hmac-sha**

- Use the **no** version to reset the transform to the default, esp-3des-hmac-sha.

Monitoring DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec Tunnels

This section contains information about troubleshooting and monitoring DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec tunnels.

System Event Logs

To troubleshoot and monitor DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec tunnels, use the following system event log:

- itm—IPSec transport mode

For more information about using event logs, see the *JUNOSe System Event Logging Reference Guide*.

show Commands

To display profile and connection information for DVMRP/IPSec, GRE/IPSec, and L2TP/IPSec tunnels, use the following **show** commands.

show dvmrp tunnel
show gre tunnel

- Use to display information about DVMRP or GRE tunnels.
- If the tunnel is protected by IPSec, the **show dvmrp tunnel detail** and **show gre tunnel detail** commands include a line indicating the IPSec transport interface. The line is not shown for unsecured tunnels. The following is a partial display. See *Monitoring IP Tunnels* in *Chapter 10, Configuring IP Tunnels* for full descriptions of the commands.
- Example

```
host1#show gre tunnel detail
Tunnel operational configuration
  Tunnel name is 'vr1'
  Tunnel mtu is '10240'
  Tunnel source address is '10.0.0.2'
  Tunnel destination address is '10.0.0.1'
  Tunnel transport virtual router is vr1
  Tunnel checksum option is disabled
  Tunnel up/down trap is enabled
  Tunnel server location is 4/0
  Tunnel secured by ipsec transport interface 1
  Tunnel administrative state is up
. . .
```

show ipsec ike-sa
show ike sa

NOTE: The **show ipsec ike-sa** command replaces the **show ike sa** command, which may be removed completely in a future release.

- Use to display IKE phase 1 SAs running on the router.
- When NAT-T is enabled on both the client PC and the E-series router, and the router has negotiated NAT-T as part of the IKE SA, the local UDP port number displayed in the Local:Port column is typically 4500. When NAT-T is disabled or not supported on one or both sides of the IKE SA negotiation, the local UDP port number is 500. (See the *Example* on page 327 for more information.)
- Field descriptions
  - Local:Port—Local IP address and UDP port number of phase 1 negotiation
  - Remote:Port—Remote IP address and UDP port number of phase 1 negotiation
  - Time(Sec)—Time remaining in phase 1 lifetime, in seconds
  - State—Current state of the phase 1 negotiation. Corresponds to the messaging state in the main mode and aggressive mode negotiations. Possible states are:
    - AM_SA_I—Initiator has sent initial aggressive mode SA payload and key exchange to the responder
    - AM_SA_R—Responder has sent aggressive mode SA payload and key exchange to the initiator
    - AM_FINAL_I—Initiator has finished aggressive mode negotiation
    - AM_DONE_R—Responder has finished aggressive mode negotiation
    - MM_SA_I—Initiator has sent initial main mode SA payload to the responder
    - MM_SA_R—Responder has sent a response to the initial main mode SA
    - MM_KE_I—Initiator has sent initial main mode key exchange to the responder
    - MM_KE_R—Responder has sent a response to the key exchange
    - MM_FINAL_I—Initiator has sent the final packet in the main mode negotiation
    - MM_FINAL_R—Responder has finished main mode negotiation
    - MM_DONE_I—Initiator has finished main mode negotiation
    - DONE—Phase 1 SA negotiation is complete, as evidenced by receipt of some phase 2 messages
  - Local Cookie—Unique identifier (SPI) for the local phase 1 IKE SA
  - Remote Cookie—Unique identifier (SPI) for the remote phase 1 IKE SA

- Example

  The following example displays the IKE phase 1 SAs for three remote client PCs that are accessing an E-series router (IP address 21.227.9.8).

  The first client PC listed (IP address 21.227.9.10) is *not* located behind a NAT device, and is therefore not using NAT-T to access the router. This PC appears in the Remote:Port column with its own IP address (21.227.9.10) and UDP port number 500.

  The remaining two client PCs are located behind a NAT device that has IP address 21.227.9.11, and are using NAT-T to access the router. These PCs appear in the Remote:Port column with the same IP address (21.227.9.11) but with two different UDP port numbers, 4500 and 14500.

```
host1#show ipsec ike-sa

IKE Phase 1 SA's:
Local:Port            Remote:Port           Time(Sec) State       Local Cookie       Remote Cookie
21.227.9.8:500        21.227.9.10:500       26133     DONE        0x87a943562124c711 0xafa2cf4a260399a4
21.227.9.8:4500       21.227.9.11:4500      28774     DONE        0x01f9efa234d45ad8 0xada4cb7cafee9243
21.227.9.8:4500       21.227.9.11:14500     28729     DONE        0x0c5ccb6b94b00051 0xe975c0ae3b9ca8bf
```

show ipsec option

- Use to display whether NAT-T is enabled or disabled on the current virtual router.
- The **show ipsec option** command also displays the status of dead peer detection (DPD) on the virtual router. For information about configuring and monitoring DPD, see *Chapter 6, Configuring IPSec*.
- Example

```
host1:westford#show ipsec option

IPsec options:
Dead Peer Detection: disabled
NAT Traversal      : enabled
```

show ipsec transport interface

- Use to display information about transport connections.
- Field descriptions
  - IPSec transport interface—Number and status of the IPSec transport connection
  - Configuration
    - Virtual router—Virtual router on which this profile is configured
    - Application—Type of application the connection can protect
    - pfs group—PFS group being used for the connection
    - Mtu—Tunnel's MTU size
    - Local address—Local endpoint address
    - Remote address—Remote endpoint address
    - Local identity—Shows the subnet, protocol, and port

- Remote identity—Shows the subnet, protocol, and port
- Inbound spi—Inbound security parameter index
- Inbound transform—Inbound algorithm
- Inbound lifetime—Inbound configured lifetime in seconds and kilobytes
- Outbound spi—Outbound security parameter index
- Outbound transform—Outbound algorithm
- Outbound lifetime—Outbound configured lifetime in seconds and kilobytes

- Statistics
  - InUserPackets—Number of user packets received
  - InUserOctets—Number of octets received from user packets
  - InAccPackets—Number of encapsulated packets received
  - InAccOctets—Number of octets received in encapsulated packets
  - InAuthErrors—Number of authentication errors received
  - InReplyErrors—Number of reply errors in received traffic
  - InPolicyErrors—Number of policy errors in received traffic
  - InOtherRxErrors—Number of packets received that have errors other than those listed above
  - InDecryptErrors—Number of decryption errors in received traffic
  - InPadErrors—Number of packets received that had invalid values after the packet was decrypted
  - OutUserPackets—Number of user packets sent
  - OutUserOctets—Number of octets sent in user packets
  - OutAccPackets—Number of encapsulated packets sent
  - OutAccOctets—Number of octets sent in encapsulated packets
  - OutPolicyErrors—Number of packets arriving at the transport connection for encapsulation that do not meet the specified identifier (selector)
  - OutOtherTxErrors—Number of outbound packets that have errors other than those listed above

- Example 1

```
host1:vr11#show ipsec transport interface
IPSEC transport interface 5 is Up
IPSEC transport interface 6 is Up
2 Ipsec transport interfaces found
```

- Example 2

```
host1:vr11#show ipsec transport interface 5
IPSEC transport interface 5 is Up
```

- Example 3

```
host1:vr11#show ipsec transport interface detail 5
IPSEC transport interface 5 is Up
  Configuration
    Virtual router vr00
    Application gre
    No pfs group
    Mtu is 1440
    Local address is 10.255.0.61
    Remote address is 10.255.0.62
    Local identity is subnet 10.255.0.61 255.255.255.255, proto 47, port 0
    Remote identity is subnet 10.255.0.62 255.255.255.255, proto 47, port 0
    Inbound spi 0x15c30204
    Inbound transform transport-esp-3des-sha1
    Inbound lifetime 900 seconds 102400 kilobytes
    Outbound spi is 0x16a10205
    Outbound transform transport-esp-3des-sha1
    Outbound lifetime 900 seconds 102400 kilobytes

  Statistics
    InUserPackets           5
    InUserOctets            270
    InAccPackets            5
    InAccOctets             440
    InAuthErrors            0
    InReplayErrors          0
    InPolicyErrors          0
    InOtherRxErrors         0
    InDecryptErrors         0
    InPadErrors             0

    OutUserPackets          5
    OutUserOctets           270
    OutAccPackets           5
    OutAccOctets            440
    OutPolicyErrors         0
    OutOtherTxErrors        0
```

show ipsec transport interface summary

- Use to display a summary of existing IPSec transport connections by application and state.
- Field descriptions
  - up—Number of IPSec transport interfaces that are currently up
  - down—Number of IPSec transport interfaces that are currently down
  - upper-bound—Number of IPSec transport interfaces that are currently bound to the upper layer
- Example

```
host1:vr11#show ipsec transport interface summary
Operational status       up         down       upper-bound
                         2          0          2
```

show ipsec transport profile

- Use to display the configuration of an IPSec transport profile.
- Field descriptions
  - IPSec transport profile—Name of the profile
    - Virtual router—Virtual router on which this profile is configured
    - Peer address—Remote endpoint address
    - Application—Type(s) of application that this profile is protecting
    - Lifetime range in seconds—Lifetime range in seconds configured for the profile
    - Lifetime range in kilobytes—Lifetime range in kilobytes configured for the profile
    - TransformSet—Transform set(s) configured for the profile
    - Pfs group—PFS group configured for the profile; 0 (zero) means that PFS is not configured for the profile
    - Local ip address—Local endpoint address
- Example 1

```
host1:vr11#show ipsec transport profile
IPSEC transport profile goi1
IPSEC transport profile goi2
2 Ipsec transport profiles found
```

- Example 2

```
host1:vr11#show ipsec transport profile goi1
IPSEC transport profile goi1
  Virtual router vr00
  Peer address 10.255.0.62
  Application gre,dvmrp
  Lifetime range in seconds 900 900
  Lifetime range in kilobytes 102400 4294967294
  TransformSet transport-esp-3des-sha1
  Pfs group 0
  Local ip address : 10.255.0.61
```

show l2tp destination profile

- Use to display configuration information for an L2TP destination profile and its associated L2TP host profiles.
- If single-shot tunnels are configured for a particular host profile, the command displays this information as an attribute of the profile for that remote host.
- Field descriptions
  - Destination profile attributes:
    - Transport—Method used to transfer traffic
    - Virtual router—Name of the virtual router
    - Peer address—IP address of the LAC

- Destination profile maximum sessions—Maximum number of sessions allowed for the destination profile
- Destination profile current session count—Number of current sessions for the destination profile

- Host profile attributes:
  - Remote host is—Name of the remote host
  - Tunnel password is—Password for the tunnel
  - Interface profile is—Name of the host profile
  - Local host name is—Name of the local host
  - Ipsec transport is—Status of the IPSec transport connection: enabled or disabled
  - Disconnect-cause avp is—Status of the disconnect cause AVP generation: enabled or disabled
  - Tunnels are single-shot—Indicates that single-shot tunnels are configured for this host profile
  - Current session count is—Number of current sessions for the host profile

- Example

```
host1#show l2tp destination profile westford
L2TP destination profile westford
Configuration
  Destination address
    Transport ipUdp
    Virtual router default
    Peer address 172.31.1.99
Statistics
  Destination profile current session count is 1
Host profile attributes
  Remote host is lac-1
    Configuration
      Tunnel password is password
      Interface profile is tunneled-user
      Local host name is lns-1
      Ipsec transport is enabled
      Disconnect-cause avp is enabled
      Tunnels are single-shot
    Statistics
      Current session count is 1
1 L2TP host profile found
```