

4

Configuring L2TP

Layer Two Tunneling Protocol (L2TP) is a client-server protocol that allows Point-to-Point Protocol (PPP) to be tunneled across a network. This chapter provides information for configuring L2TP in your ERX system.

Topic	Page
Overview	4-1
Before You Configure the LAC or LNS	4-6
Configuring the LAC	4-6
Configuring the LNS	4-14
Enabling Tunnel Switching	4-17
Creating Persistent Tunnels	4-20
Testing Tunnel Configuration	4-21
Managing L2TP	4-21
Monitoring Tunnels and Sessions	4-23

Overview

L2TP encapsulates layer 2 packets, such as PPP, for transmission across a network. An L2TP Access Concentrator (LAC), configured on an access device, such as an ERX edge router, receives packets from a remote client and forwards them to an L2TP Network Server (LNS), on a remote network.

You can configure your ERX system to act as an LAC in pass-through mode in which the LAC receives packets from a remote client and then forwards them at layer 2 directly to the LNS.

The ERX system creates tunnels dynamically by using AAA authentication parameters and transmits L2TP packets to the LNS via Internet Protocol (IP)/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*. A tunnel is an aggregation of one or more sessions. Figure 4-1 and Figure 4-2 show a typical arrangement.

You can configure an ERX system to act as an LAC.

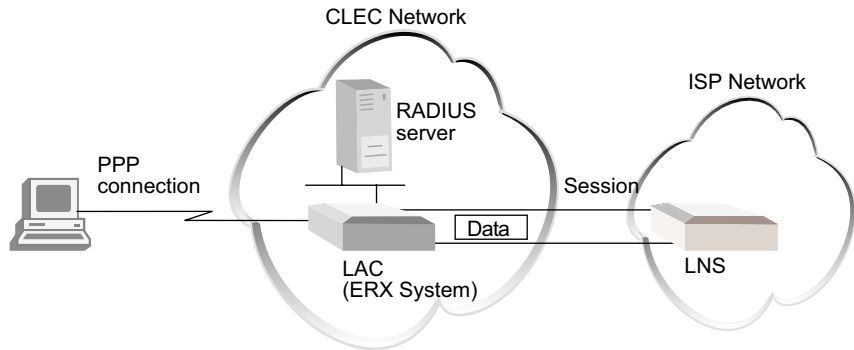


Figure 4-1 Using the ERX system as an LAC

You can also configure an ERX system to act as an LNS.

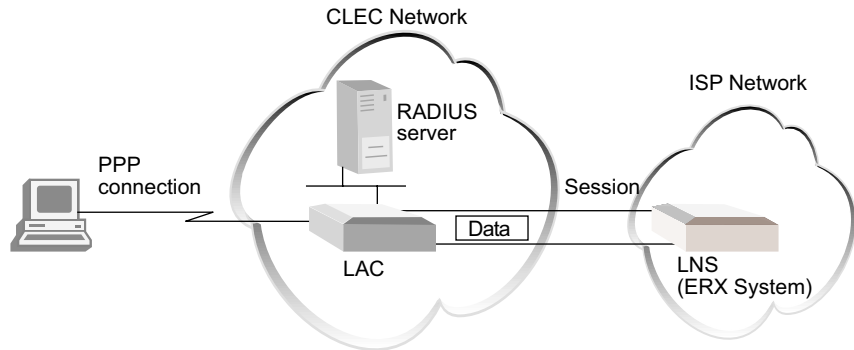


Figure 4-2 Using the ERX system as an LNS



Note: The ERX system does not support terminating both ends of a tunnel or session in the same router.

References

For more information about the L2TP protocol, consult the following resource: RFC 2661 – Layer Two Tunneling Protocol “L2TP” (August 1999)

Terminology

Table 4-1 defines the basic terms for L2TP.

Table 4-1 L2TP terms

Term	Meaning
Attribute value pair (AVP)	Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
L2TP access concentrator (LAC)	A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. An LAC sits between an LNS and a remote system and forwards packets to and from each.
Call	A connection (or attempted connection) between a remote system and an LAC.
L2TP network server (LNS)	A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. The logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
Peer	In the L2TP context, refers to either the LAC or LNS. An LAC's peer is an LNS, and vice versa.
Remote system	An end-system or router attached to a remote access network, which is either the initiator or recipient of a call.
Session	A logical connection created between the LAC and the LNS when an end-to-end PPP connection is established between a remote system and the LNS. Note: <i>There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.</i>
Tunnel	A connection between an LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

Implementing L2TP

The implementation of L2TP for the ERX system uses four levels:

- *System* – the ERX system
- *Destination* – the remote L2TP system
- *Tunnel* – a direct path between the LAC and the LNS
- *Session* – a PPP connection in a tunnel

When the ERX system has established destinations, tunnels, and sessions, you can control the L2TP traffic. Making a change to a destination affects all tunnels and sessions to that destination; making a change to a tunnel affects all sessions in that tunnel. For example, closing a destination closes all tunnels and sessions to that destination.

Sequence of Events on the LAC

The ERX system creates destinations, tunnels, and sessions dynamically, as follows:

- 1 The client initiates a PPP connection with the system.
- 2 The system and the client exchange Link Control Protocol (LCP) packets.



Note: See the *ERX Physical and Link Layers Configuration Guide, Chapter 13, Configuring Point-to-Point Protocol* for details about negotiating PPP connections.

- 3 By using either a local database related to the domain name or RADIUS authentication, the ERX system determines either to terminate or to tunnel the PPP connection.
- 4 If the system discovers that it should tunnel the session, it does the following:
 - a Sets up a new destination or selects an existing destination.
 - b Sets up a new tunnel or selects an existing tunnel.
 - c Opens a new session.
- 5 The system forwards the results of the LCP negotiations and authentication to the LNS.

A PPP connection now exists between the client and the LNS.



Note: The ERX system discards received packets if the size of the variable-length, optional offset pad field in the L2TP header is too large. The ERX system always supports packets that have an offset pad field of up to 16 bytes, and may support larger offset pad fields, depending on other information in the header. This restriction is a possible, although unlikely, cause of excessive discarding of L2TP packets.

Sequence of Events on the LNS

The ERX system sets up an LNS as follows:

- 1 An LAC initiates a tunnel with the system.
- 2 The system verifies that a tunnel with this LAC is valid—destination configured, host name and tunnel password correct.
- 3 The system completes the tunnel setup with the LAC.
- 4 The LAC sets up a session with the system.
- 5 The system creates a dynamic PPP interface on top of the session.

- 6 If they are enabled and present, the system takes the proxy LCP and the proxy authentication data and passes them to PPP.
- 7 The ERX PPP processes the proxy LCP, if it is present, and, if acceptable, places LCP on the system in opened state without renegotiation of LCP.



Note: If proxy LCP is not present or not acceptable, the ERX system negotiates LCP with the remote system.

- 8 The ERX PPP processes the proxy authentication data, if it is present, and passes the data to AAA for verification. (If the data is not present, ERX PPP requests the data from the remote system.)
- 9 The system passes the authentication results to the remote system.

Packet Fragmentation

The ERX system supports the reassembly of IP-fragmented L2TP packets. (See *ERX Routing Protocols Configuration Guide, Vol. 1, Chapter 5, IP Reassembly for Tunnels*, for more information.) However, it is preferable to prevent fragmentation within L2TP tunnels because of the effects of fragmentation and reassembly on performance.

To prevent fragmentation, PPP LCP negotiation of the maximum receive unit (MRU) may be used to determine a proper maximum transmission unit (MTU). However, the normal automatic method of determining the proper MRU to negotiate (by evaluating the MRU of all lower layers in the interface stack) is not adequate for L2TP. The initial LCP negotiation between PPP in the client and the LAC is inadequate because it does not cover the entire extent of the eventual PPP session that travels all the way from the client to the LNS. Furthermore, even if PPP in the LNS chooses to renegotiate the MRU, it has no way to determine the proper MRU, since it does not know the minimum MRU on all of the intervening links between it and the LAC.

To overcome the inadequacy of normal determination of the MRU under such circumstances, the ERX system supports a configurable PPP MRU via the following command:

```
host1(config-if)#ppp mru size  
host1(config-profile)#ppp mru size
```

This command may be specified at either the LAC or LNS. When specified at the LAC, it should be specified in the Interface Configuration mode when you are configuring the relevant PPP interface. When specified at the LNS, it should be specified in the Profile Configuration mode when you are configuring dynamic PPP interfaces. The size

specified must take into account the MRU for all possible links between the LAC and the LNS. It must also take into account the L2TP encapsulation that is added to all packets entering the tunnel. For example, if the link between the LAC and LNS with the lowest MRU were an Ethernet link, the following calculation would apply:

Minimum link MRU	1500
L2TP encapsulating IP header	-20
L2TP encapsulating UDP header	-8
Maximum L2TP header*	-30
MRU size to specify	1442
* Assumes a maximum of 16 bytes of Offset Pad.	

Specifying **ppp mru 1442** at either the LAC or LNS guarantees that no fragmentation will occur within the L2TP tunnel.

Before You Configure the LAC or LNS

Before you begin configuring your ERX system as an LAC:

- 1 Create a virtual router.

```
host1(config)#virtual-router west
```

- 2 Assign an IP address, such as that for a loopback interface, to the virtual router. For example:

```
host1:westboro(config)#ip router-id 10.10.45.3
```



Note: Step 2 is not necessary if you have set the source-address option discussed later in this chapter.

- 3 Configure the ERX system or virtual router for B-RAS.

Configuring the LAC

A single ERX system may function as an LAC for some tunnels and an LNS for others, but your ERX system does not support termination at both ends of the *same* tunnel or session in the *same* router.

The ERX system supports ingress and egress rate limiting on PPP traffic bound for L2TP tunnels. You can apply rate limits per L2TP session. To apply rate limits in this configuration, you must define an unnumbered IP interface above the PPP connection on the ingress interface. Apply rate limits to this IP interface as described in *ERX Policy and QoS*

Configuration Guide, Chapter 1, Configuring Policy Management. Rate limits affect the IP-routed traffic when PPP is terminated and affect the PPP traffic when PPP is tunneled. All traffic is rate limited; you cannot exclude PPP control traffic.



Note: When you use dynamic profiles to apply rate limits to PPP traffic that is tunneled over L2TP, you must specify a VR in the profile to give the interface stack a context in which to be created.

The ERX system can initiate L2TP tunnels based either on a locally configured domain map or RADIUS profile information. In either case, the data is selected by domain name.

You can create a system-wide maximum of 16,000 sessions spread in any combination across a maximum of 4,000 tunnels shared between an LAC and an LNS. This means that if an ERX system is operating as an LAC for some tunnels and as an LNS for others, the 4,000 tunnels and 16,000 sessions limit applies to the combined total of LAC and LNS tunnels and sessions.

LACs support the creation of VLANs on the Fast Ethernet (FE) and Gigabit Ethernet (GE) modules. See *ERX Physical and Link Layers Configuration Guide, Chapter 6, Configuring Ethernet Interfaces* for additional information on VLANs.

Modules Supported by the LAC

Table 4-2 lists the line modules supported by an LAC. The table also indicates the kind of support each module type receives. There are two sides to the LAC support: the access side and the peer side. The access side provides access to the L2TP client; the peer side provides support for the L2TP uplink to the LNS.

Table 4-2 Line modules and LAC support

Module Type	Access Side	Peer Side
Dual-port OC3	yes	yes
FE-2	yes	yes
FE-8	yes	yes
GE	yes	yes
OCx/STMx ATM	yes	yes
OCx/STMx POS	no	yes
T3 ATM	yes	yes

l2tp checksum

- Use to enable the checking of data integrity via UDP.
- Checksum is always used for L2TP control traffic.
- Example

```
host1(config)#l2tp checksum
```
- Use the **no** form to disable UDP checksum (the default).

l2tp destruct-timeout

- Use to specify the maximum time period, in the range 10–3600 seconds (1 hour), for which the ERX system attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
- Any specific dynamic destination, tunnel, or session may not be maintained for this entire time period if the resources must be reclaimed early to allow new tunnels to be established.
- Example

```
host1(config)#l2tp destruct timeout 1200
```
- Use the **no** form to set this time to the default, 600 seconds (10 minutes).

l2tp retransmission

- Use to specify the number of retransmission retries, in the range 2–7.
- Example

```
host1(config)#l2tp retransmission 4
```
- Use the **no** form to set the retransmission retry count to the default, 5.

Mapping a User Domain Name to an L2TP Tunnel

When a client initiates a PPP connection with the ERX system, the client and the ERX system exchange Link Control Protocol (LCP) packets to negotiate the characteristics of the session.

Using either the local database related to the domain name or a RADIUS server, the ERX system determines whether or not to terminate or tunnel the PPP connection.

If the ERX system discovers that it should tunnel the session, it does the following: (1) either sets up a new destination or selects an existing destination; (2) either sets up a new tunnel or selects an existing tunnel; and (3) opens a new session. The ERX system forwards the result of the LCP negotiations and authentication to the LNS.

See *ERX Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access to the ERX System* for information on setting up RADIUS to provide this mapping.



Note: This section applies to the LAC, not to the LNS. Do not specify a domain map at the LNS. If you do so, the PPP connections for that domain will fail.

To map a domain to an L2TP tunnel locally on the ERX system:

- 1 Specify a domain name.

```
host1(config)#aaa domain-map westford.com
```

- 2 Specify a virtual router; in this case, the *default* router is specified.

```
host1(config-domain-map)#virtual-router default
```

- 3 Specify a tunnel to configure.

```
host1(config-domain-map)#tunnel 3
```

- 4 Specify the LNS endpoint address of a tunnel.

```
host1(config-domain-map-tunnel)#address 172.31.1.98
```

- 5 Specify a preference for the tunnel.

```
host1(config-domain-map-tunnel)#preference 5
```

- 6 (Optional) Specify an authentication password.

```
host1(config-domain-map-tunnel)#password temporary
```



Note: If you specify a password for the LAC, your ERX system requires that the peer (the LNS) authenticate itself to the system. In this case, if the peer fails to authenticate itself, the tunnel terminates.

- 7 (Optional) Specify a host name for the LAC end of the tunnel.

```
host1(config-domain-map-tunnel)#client-name host4
```

- 8 (Optional) Specify a server name for the LNS.

```
host1(config-domain-map-tunnel)#server-name boston
```

- 9 (Optional) Specify a source IP address for the LAC tunnel endpoint.

```
host1(config-domain-map-tunnel)#source-address 172.23.2.74
```

- 10 Specify a tunnel identification. (The ERX system groups L2TP sessions with the same tunnel identification into the same tunnel.)

```
host1(config-domain-map-tunnel)#identification acton
```

- 11 Specify a tunnel type.

```
host1(config-domain-map-tunnel)#type l2tp
```

- 12 Specify a medium type. (Only IP version 4 is supported for PPP.)

```
host1(config-domain-map-tunnel)#medium ipv4
```

- 13 (Optional) Specify a default tunnel client name.

```
host1(config-domain-map-tunnel)#exit
host1(config-domain-map)#exit
host1(config)#aaa tunnel client-name boxford
```

- 14 (Optional) Specify a default tunnel password.

```
host1(config)#aaa tunnel password 3&92k%b#q4
host1(config)#exit
```

- 15 (Optional) Set the format for the tunnel assignment ID.

```
host1(config)#aaa tunnel assignment-id-format assignmentID
```



Note: If you do not set the tunnel assignment ID, the software sets it to default.

- 16 (Optional) Set up the system to ignore sequence numbers in data packets received on L2TP tunnels.

```
host1(config)#l2tp ignore-receive-data-sequencing
```

- 17 Verify the L2TP tunnel configuration.

```
host1#show aaa domain-map
Domain: NONE; virtual-router: default
Domain: westford.com; virtual-router: default
Tunnel          Tunnel          Tunnel Tunnel  Tunnel   Tunnel
Tag   Tunnel Peer   Source          Type   Medium  Password  Id
-----
3      172.31.1.98  172.23.2.74    l2tp   ipv4    temporary tunnel2

                Tunnel
Tunnel Tunnel Server  Tunnel
Tag   Hostname Name  Preference
-----
3      ERX4    boston 5

host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is boxford
```

aaa tunnel assignment-id-format

- Use to determine the value of the tunnel assignment ID that is passed to PPP/L2TP.
- The tunnel assignment ID format can be either only assignmentID or clientAuthId + serverAuthId + assignmentId.
- If you do not set a tunnel assignment ID, the software sets it to default. This parameter is only used by the L2TP LAC device, and the tunnel-assignment-id is generated only by the L2TP LAC device.

aaa tunnel client-name

- Use to specify a default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default name.
- Use the **no** version to delete the client name.

aaa tunnel ignore

- Use to specify whether or not the tunnel peer's NAS-Port [5] and NAS-Port-Type [61] attributes should be used. When enabled, the attribute is supplied by the tunnel peer. When disabled, the attribute is not supplied.
- Use the **no** version to negate the command or restore the default of enable.

aaa tunnel password

- Use to specify a default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default password.
- Use the **no** version to delete the tunnel password.

address

- Use to set the LNS endpoint address of a tunnel.
- Use the **no** version to remove the address of the tunnel.

client-name

- Use to specify the host name that the LAC uses when communicating to the LNS about the tunnel.
- The host name is sent to the LNS.
- The host name can be up to 64 characters long (no spaces).
- Use the **no** version to remove the host name.



Note: *If the LNS does not accept tunnels from unknown hosts, the host name must be specified to establish a tunnel. If no host name is specified, the LAC uses the system name as the host name.*

identification

- Use to specify the ID of a tunnel.
- The ERX system groups users with the same tunnel ID in the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.
- Use the **no** version to remove the assignment ID from the tunnel.

l2tp ignore-receive-data-sequencing

- Use to prevent sequence number checking for data packets received on all L2TP tunnels in the system. This command does not affect the insertion of sequence numbers in packets sent from the system.

- We recommend that you set up the system to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly may reorder L2TP packets, out-of-order packets may be dropped if sequence numbers are being used on L2TP data packets.
- Use the **no** version to cause the system to check sequence numbers on received L2TP data packets.

medium ipv4

- Use to specify the type of medium for a tunnel.
- The only medium type supported for this release is IPv4.
- Use the **no** version to set the medium to the default, IPv4.

password

- Use to specify the password for a tunnel.
- If you specify a password, your ERX system (the LAC) requires that the peer (the LNS) authenticate itself to the system.
- If the peer fails to authenticate itself, the tunnel terminates.

preference

- Use to specify the preference level for a tunnel.
- You can specify up to eight levels of preference for the ERX system.
- You can assign the same preference to a maximum of eight tunnels.
- When you define multiple preferences for a destination, you increase the probability of a successful connection.
- Use the **no** version to set the preference number from the tunnel to the default, 0.

server-name

- Use to specify the host name expected from the peer (the LNS) when you set up a tunnel.
- When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated.
- The server name can be up to 64 characters long (no spaces).
- Use the **no** version to remove the server name.

source-address

- Use to specify the address of the local tunnel endpoint (the LAC).
- When this address is specified, all L2TP packets transmitted to the peer use this address.
- If this address is not specified, the virtual router's router ID is used as the source address.
- Use the address of a stable IP interface (for example, a loopback interface). The address should also be an IP address in the specified virtual router for this domain map.
- Use the **no** version to remove the source address.

tunnel

- Use to specify a tunnel and to enter Domain Map Tunnel Configuration mode.
- Use the **no** version to delete the tunnel configuration.
- If a password is specified, the same password must be configured at both the LAC and the LNS.
- Use the **no** version to remove the password from the tunnel.

type

- Use to specify the type of a tunnel as L2TP.
- Use the **no** version to set the tunnel type to the default, L2TP.

LNS Round-Robin Selection

L2TP allows you to specify:

- Up to 31 destinations for a domain
- Up to eight levels of *preference* for the ERX system
- Up to eight destinations for a preference

Preference indicates the order in which the system attempts to connect to the destinations specified for a domain. The system makes up to eight attempts to connect to a destination for a domain—one attempt for each level of preference. Zero (0) is the highest level of preference. If a destination is found to be unreachable, it is marked as such and is not tried again for five minutes.

When you try to log into your domain, the system attempts to connect to a destination with the highest preference. At each level of preference, if there is a single destination that is not considered unreachable, the system attempts to contact that destination. If there is more than one destination that is not considered unreachable, the system randomly selects a destination and attempts to contact it.

The random selection approximates a round-robin selection mechanism. If there are no destinations considered unreachable at a given level, the system chooses the destination that failed first. The key is to understand that the system chooses a single destination at each level of preference, even if all destinations have recently failed. Thus the 5-minute timer normally used to reinstate failed destinations is ignored under certain conditions.

If the destination chosen at a level of preference fails, the system goes on to the next level of preference, continuing until eight attempts have been made.

For example, suppose you have three destinations for a domain: A, B, and C. You assign the following preferences:

- A, B, and C at preference 0
- A, B, and C at preference 1
- A, B, and C at preference 2

A, B, and C are all considered reachable.

If you try to connect to the domain, suppose the system randomly selects destination A from preference 0. If this connection attempt fails, the system excludes destination A for 5 minutes and goes to the next level (preference 1). From here, it randomly selects destination B, one of the two remaining choices. If the second connection attempt also fails, the system excludes destination B, as well as destination A, and attempts to connect to destination C, the only destination available with preference 2. The system has had an opportunity to connect to every destination available for the domain.

Support for multiple destinations affects the procedure for mapping a user domain name to an L2TP tunnel. To learn how to complete this mapping, see *Mapping a User Domain Name to an L2TP Tunnel* earlier in this chapter.

Configuring the LNS

When you configure an LNS, you can configure it to accept calls from any LAC.



Note: If there is no explicit LNS configuration on the ERX system, the UDP port used for L2TP traffic is closed, and no tunnels or sessions can be established.

You must create two objects on the ERX system to enable an LAC to connect to the LNS:

- An L2TP destination profile – defines the location of the LAC(s)
- An L2TP host profile – defines the attributes used when communicating with an LAC

l2tp destination profile

- Use to create the destination profile that defines the location of the LAC.
- This command accesses the 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 ERX system currently supports a maximum of 4,000 L2TP destination profiles.
- Example

```
host1:boston(config)#l2tp destination profile boston ip
address 10.10.76.12
```

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



Note: When you remove a destination profile, you remove all the tunnels and sessions using that profile.

remote host

- Use to define the L2TP host profile.
- Each L2TP destination profile can have multiple L2TP host profiles.
- For an LAC to connect to an LNS, the appropriate L2TP destination profile *must* have at least one L2TP host profile.
- If any name other than *default* is specified for the remote host, then the LAC must supply the specified host name in order for the tunnel to be set up. The remote host name is matched against the host name AVP in the received Start-Control-Connection-Request (SCCRQ).
- The remote host name can be up to 64 characters long (no spaces).
- Example 1

```
host1:boston(config)#l2tp destination profile boston1 ip
address 192.168.76.12
host1:boston(config-l2tp-dest-profile)#remote host default
```

- Example 2

```
host1:boston(config)#l2tp destination profile boston2 ip
address 192.168.76.15
host1:boston(config-l2tp-dest-profile)#remote host xyz
```

- Use the **no** version to remove the L2TP host profile.



Note: When you remove a host profile, you terminate all the tunnels and sessions using that profile.

Host Profile Attributes

Each L2TP host profile has a set of attributes you can modify. The following commands allow you to modify host profile attributes.

disable proxy lcp

- Use to disable the use of proxy LCP when connecting to the selected host.
- Default is proxy LCP enabled.

enable proxy authenticate

- Use to enable the use of proxy authentication when connecting to the selected host.
- Default is proxy authenticate disabled.

local host

- Use to specify the local host name to be used in any host name AVP sent to the LAC.
- Default is the system name.

local ip address

- Use to specify the local IP address to be used in any packets sent to the LAC.
- Default is the virtual router's router ID.

tunnel password

- Use to specify the shared secret to be used to authenticate the tunnel. The same password must be specified at both ends of the tunnel.
- Default is no password. (This results in no tunnel authentication.)

Here are three examples that illustrate the L2TP host profile's attributes supported by these commands:

- Example 1

```
host1:boston(config)#l2tp destination profile boston3 ip
address 192.168.76.18
host1:boston(config-l2tp-dest-profile)#remote host default
host1:boston(config-l2tp-dest-profile-host)#profile
boston3Profile1
host1:boston(config-l2tp-dest-profile-host)#disable proxy
lcp
```

- Example 2

```
host1:boston(config)#l2tp destination profile boston4 ip
address 192.168.76.20
host1:boston(config-l2tp-dest-profile)#remote host george
host1:boston(config-l2tp-dest-profile-host)#profile
georgeProfile1
```

```

host1:boston(config-l2tp-dest-profile-host)#local host andy
host1:boston(config-l2tp-dest-profile-host)#local ip address
192.168.23.1
host1:boston(config-l2tp-dest-profile-host)#enable proxy
authenticate

```

- Example 3

```

host1:boston(config-l2tp-dest-profile)#remote host weston
host1:boston(config-l2tp-dest-profile-host)#profile
westonProfile
host1:boston(config-l2tp-dest-profile-host)#local host acton
host1:boston(config-l2tp-dest-profile-host)#tunnel password
saco

```

Modules Supported by the LNS

Table 4-3 lists the line modules supported by the LNS. The table also indicates the kind of support each module type receives. There are two sides to the LNS support: the internet side and the peer side. The internet side must be a tunnel server card; the peer side provides support for the L2TP uplink to the LAC.

Table 4-3 Line modules and LNS support

Module Type	Internet Side	Peer Side
Dual-port OC3	no	yes
FE-2	no	yes
GE	no	yes
OCx/STMx ATM	no	yes
OCx/STMx POS	no	yes
T3 ATM	no	yes
Tunnel Service	yes	yes



Note: To use an LNS, there must be at least one Tunnel Service module in the ERX system.

Enabling Tunnel Switching

L2TP tunnel switching allows you to switch packets between one session terminating at an L2TP LNS and another session originating at an L2TP LAC. What distinguishes a tunnel-switched LAC from a conventional one is that the LAC session is layered above an LNS session in the interface stack.



Note: The LAC session can either reside immediately above the LNS session, or there can be intervening layer 2 interfaces between the LAC and the LNS.

You can select tunnel switching on a per-chassis basis. By default, tunnel switching is disabled. This preserves current behavior and prevents inadvertent attempts to switch tunnels.



Note: Each individual L2TP session involved in tunnel switching is counted toward the maximum number of sessions supported on an ERX system.

I2tp tunnel-switching

- Use to enable tunnel switching.
- Use the **no** version to disable tunnel switching. This is the default setting.

Enabling Tunnel Selection

This section presents three new capabilities to the LAC's tunnel selection process. Previously, when the ERX LAC determined that a PPP session should be tunneled, the system selected a tunnel from among a set of tunnels associated with either the PPP user or the PPP user's domain. This method of selection remains the default method of selection.

Your ERX system now supports the following alternate methods for tunnel selection:

- Tunnel selection fail-over within a preference level
- Maximum session per tunnel configuration
- Weighted load balancing

Currently, L2TP supports the following in your ERX system:

- Up to 31 tunnels for a domain
- Up to 8 levels of preference for the ERX system
- Up to 8 tunnels at the same preference level

Enabling Tunnel Selection Failover Within a Preference Level

In this failover method, when an attempt to connect to a tunnel fails, a new tunnel at the same preference level is selected. After attempting to connect to all reachable tunnels at a given preference level, a tunnel is selected from the next lower level.

At any preference level where more than one reachable tunnel is defined, the next tunnel to contact is selected randomly. If all tunnels at a preference level are marked as unreachable, the system drops down to the

next lower preference level to select a tunnel. If all tunnels at all preference levels are found to be unreachable, the system rejects the PPP user session without attempting to contact the remote system.

If your ERX system randomly selects a tunnel from a preference level when trying to connect to a domain, and that tunnel connection attempt fails, the system selects another tunnel at the same preference level. This method of selecting tunnels differs from the default method in which, when a tunnel selected at the preference level fails, the system then selects from the next preference level even if there are available tunnels at the first preference level.

l2tp fail-over-within-preference

- Use to enable tunnel selection within a preference level.
- Example

```
host1(config)#l2tp fail-over-within-preference
```
- Use the **default** version to drop down a preference level when a connection attempt fails.
- Use the **no** version to disable this feature.

Configuring Maximum Sessions per Tunnel

This feature enables the maximum number of sessions to be configured on a per tunnel basis, either through your RADIUS server or the command line interface (CLI). The maximum sessions tunnel attribute is considered when selecting a tunnel for a PPP session. If a randomly selected tunnel has a current session count equal to its maximum session count, no attempt is made to contact that tunnel. Instead, an alternate tunnel selection is made from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the system drops down a preference level to make the next selection. This process is consistent, regardless of which fail-over scheme is currently running on the system. A tunnel without a configured maximum sessions value, is considered to have no upper bound on the number of sessions it can support.

max-sessions

- Use to configure the maximum sessions per tunnel.
- Example

```
host1(config)#aaa domain-map lacOne
host1(config-domain-map)#tunnel 1
host1(config-domain-map-tunnel)#max-sessions 1500
```

- Use the **default** version to set the value to zero. Setting the value to zero allows unlimited sessions in the tunnel.
- Use the **no** version to disable this feature.

Enabling Weighted Load Balancing

The weighted load balancing scheme is based on the maximum sessions per tunnel attribute.

Enabling this feature results in a weighted load balancing scheme being used for tunnel selection. The weight associated with a tunnel is used when choosing among multiple tunnels sharing the same preference level. The weight of a given tunnel is proportional with respect to its maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the largest weight; the tunnel with the next largest maximum session value has the next largest weight, down to the tunnel with the smallest maximum session value that has the smallest weight.

l2tp weighted-load-balancing

- Use to override the default behavior in which a session load is distributed evenly across all tunnels at the same preference level.
- Example

```
host1(config)#l2tp weighted-load-balancing
```
- Use the **default** version to return to the default behavior (described above).
- Use the **no** version to disable this feature.

Creating Persistent Tunnels

Your ERX system supports persistent tunnels. A persistent tunnel is one that is configured to remain available. Persistent tunnels have only local significance; that is, they apply only to the end of the tunnel where they are set. If the other end of the tunnel chooses to terminate the tunnel, the tunnel is removed.

l2tp tunnel idle-timeout

- Use to configure L2TP tunnel idle timeout.
- Use to create a persistent tunnel. You do this by setting the idle-timeout value to zero.
- Example

```
host1(config)#l2tp tunnel idle-timeout 0
```
- Use the **no** version to remove the idle timeout setting.

Testing Tunnel Configuration

The **l2tp tunnel test** command allows you to force the establishment of a tunnel in order to verify both the tunnel configuration and connectivity. In previous releases, you were allowed to test a tunnel configuration only by bringing up a tunneled PPP session.

l2tp tunnel test

- Use to test a tunnel's configuration and connectivity.
- This command supports tunnel initiation: incoming calls on the LAC; outgoing calls on the LNS.
- This command does not support tunnel respondent: outgoing calls on the LAC; incoming calls on the LNS.
- Examples:

```
host1#l2tp tunnel test boston.com
host1#l2tp tunnel test portland.com gold
```

Managing L2TP

Configuring an ERX system for B-RAS allows it to operate as an LAC with default settings. You can modify the default settings as follows:

- Enable the checking of data integrity via UDP.
This also applies to an LNS, but there is no default configuration that enables the LNS.
- Specify the time period for which the ERX system maintains dynamic destinations, tunnels, or sessions after termination.
This also applies to an LNS, but there is no default configuration that enables the LNS.

When the ERX system is established as an LAC or LNS and is creating destinations, tunnels, and sessions, you can manage them as follows:

- Prevent the creation of new sessions, tunnels, and destinations.
- Close and reopen all or selected destinations, tunnels, and sessions.



Note: All of the commands in this section apply to both the LAC and the LNS.

l2tp drain

- Use to prevent the creation of new destinations, tunnels, and sessions on the ERX system.
- This command and the **l2tp shutdown** command both affect the administrative state of L2TP on the system. Although each command has a different effect,

the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- Example

```
host1(config)#l2tp drain
```

- Use the **no** version to enable the creation of new destinations, tunnels, and sessions.

l2tp drain destination

- Use to prevent the creation of new tunnels and sessions at a destination.
- This command and the **l2tp shutdown destination** command both affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- Example

```
host1(config)#l2tp drain destination ip 172.31.1.98
```

- Use the **no** version to enable the creation of tunnels and sessions for a destination.

l2tp drain tunnel

- Use to prevent the creation of new sessions for a tunnel.
- This command and the **l2tp shutdown tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- Example

```
host1(config)#l2tp drain tunnel virtual-router default ip  
172.31.1.98 isp.com
```

- Use the **no** version to enable the creation of a tunnel.

l2tp retransmission

- Use to specify the number of retransmission retries.

- Example

```
host1(config)#l2tp retransmission 4
```

- Use the **no** form to set the retransmission retry count to the default, 5.

l2tp shutdown

- Use to close all destinations, tunnels, and sessions, and to prevent the creation of new destinations, tunnels, and sessions on the system.
- This command and the **l2tp drain** command both affect the administrative state of L2TP on the system. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- Example

```
host1(config)#l2tp shutdown
```
- Use the **no** version to enable the creation of new destinations, tunnels, and sessions.

l2tp shutdown destination

- Use to close all tunnels and sessions for a destination and to prevent the creation of tunnels and sessions for that destination.
- This command and the **l2tp drain destination** command both affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#l2tp shutdown destination 1
```
- Use the **no** version to enable the creation of new tunnels and sessions for a destination.

l2tp shutdown session

- Use to close selected sessions.
- Example

```
host1(config)#l2tp shutdown session 1/1/1
```
- The **no** version has no effect, because sessions can be created only dynamically at this release.

l2tp shutdown tunnel

- Use to close all sessions in a tunnel and to prevent the creation of sessions in a tunnel.
- This command and the **l2tp drain tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#l2tp shutdown tunnel 1/isp.com
```
- Use the **no** version to enable the creation of new sessions for the tunnel.

Monitoring Tunnels and Sessions

When you have configured L2TP on your ERX system, you can monitor the active tunnels and sessions.



Note: All of the commands in this section apply to both the LAC and the LNS.

show aaa tunnel-parameters

- Use to display default tunnel parameters used for tunnel definitions.
- Example

```
host1#show aaa tunnel-parameters
tunnel password is 3&92k%b#q4
tunnel client-name is boxford
tunnel nas-port-method is none
tunnel nas-port-ignore disabled
tunnel nas-port-type ignore disabled
tunnel assignmentId format is assignment
```

show l2tp

- Use to display the global configuration and status for L2TP on the ERX system, including switched sessions.
- Field descriptions
 - › Configuration:
 - L2TP administrative state – status of L2TP on the ERX system
 - Dynamic interface destruct timeout – time for which the ERX system maintains dynamic destinations, tunnels, and sessions after they have terminated
 - Data packet checksums – status of checking data integrity via UDP
 - Receive data sequencing – whether the system checks or ignores sequence numbers in incoming data packets
 - Tunnel idle timeout – length of the tunnel idle timeout
 - › Sub-interfaces:
 - total – number of destinations, tunnels, and sessions that the ERX system created
 - active – number of operational destinations, tunnels, and sessions
 - failed – number of requests that did not reach an operational state
 - auth-errors – number of requests that failed because the tunnel password was invalid
- Example

```
host1#show l2tp
Configuration
L2TP administrative state is enabled
Dynamic interface destruct timeout is 600 seconds
Data packet checksums are disabled
Receive data sequencing is not ignored
Tunnel switching is disabled
Tunnel idle timeout is 60 seconds
Sub-interfaces          total    active    failed    auth-errors
Destinations            1         1         0         n/a
Tunnels                  5         5         0         0
Sessions                 64        64        0         n/a
Switched-sessions       0         0         0         n/a
```

show l2tp destination

- Use to display detailed configuration information about specified destinations.
- Field descriptions
 - › Configuration:
 - Administrative state – configured status of the destination:
 - enabled – no restrictions on creation and operation of sessions and tunnels for this destination
 - disabled – ERX system disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
 - drain – ERX system will not create new sessions or tunnels for this destination
 - SNMP traps – whether or not the ERX system sends traps to SNMP for operational state changes
 - › Destination address:
 - Transport – method used to transfer traffic
 - Virtual router – name of the virtual router on which the tunnel is configured
 - Local and peer addresses – addresses of the local and remote interfaces
 - › Destination status:
 - Effective administrative state – the more restrictive of the ERX system and destination administrative states. This setting, rather than the administrative state of the destination, determines whether the ERX system can create new sessions or tunnels and whether the sessions or tunnels are disabled for this destination.
 - › Sub-interfaces:
 - total – number of sessions or tunnels that the ERX system created for this destination
 - active – number of operational sessions or tunnels for this destination
 - failed – number of requests that did not reach an operational state for this destination
 - auth-errors – number of requests that failed because the tunnel password was invalid for this destination
 - › Statistics – information about the traffic sent and received

- Example 1

```
host1#show l2tp destination ip 172.31.1.98
L2TP destination 1 is Up with 5 active tunnels and 64
active sessions
```

- Example 2

```
host1#show l2tp destination detail 1
L2TP destination 1 is Up with 5 active tunnels and 64
active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Destination address
  Transport ipUdp
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
Destination status
  Effective administrative state is enabled
```

Sub-interfaces	total	active	failed	auth-errors		
Tunnels	5	5	0	0		
Sessions	64	64	0	n/a		
Statistics	packets		octets		discards	errors
Control rx	69		3251		2	0
Control tx	195		23939		0	0
Data rx	68383456		68383456		0	0
Data tx	68383456		68383456		0	0

show l2tp destination profile

- Use to display either a list of configured L2TP destination profiles or the host profiles defined in a particular profile.

- Example 1

```
host1#show l2tp destination profile
L2TP destination profile acton
1 L2TP destination profile found
```

- Example 2

```
host1#show l2tp destination profile acton
L2TP destination profile acton
Destination address
Transport ipUdp
Virtual router lns
Peer address 172.31.1.99
Host profile attributes
Remote host is default
    Interface profile is bealz
Remote host is ebcdic
    Tunnel password is 111
    Interface profile is ebcints
Remote host is asciitext
    Tunnel password is 222
    Interface profile is ascints
Remote host is mexico
    Tunnel password is 333
    Interface profile is mexints
4 L2TP host profiles found
```

show l2tp destination summary

- Use to display a summary of the configured and operational status of all L2TP destinations.
- Field descriptions
 - › Administrative status:
 - enabled – no restrictions on creation and operation of sessions and tunnels for this destination
 - drain – ERX system will not create new sessions or tunnels for this destination

- disabled – ERX system disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
- › Operational status:
 - up – destination is available for tunnels
 - down – destination is not available for tunnels
 - lower-down – underlying transport is unavailable; for example, you removed the virtual router
 - not-present – hardware supporting the destination is unavailable; for example, you removed a required line module
- Example

```

host1#show l2tp destination summary
Administrative status  enabled  drain  disabled
                        1        0      0
Operational
status                up      down    lower-down  not-present
                      1        0        0          0

```

show l2tp session

- Use to display detailed configuration information about specified sessions.
- Field descriptions
 - › Configuration:
 - Administrative state – configured status of the session
 - enabled – no restrictions on the operation of this session
 - disabled – ERX system terminated this session
 - SNMP traps – whether or not the ERX system sends traps to SNMP for operational state changes
 - › Session status:
 - Effective administrative state – most restrictive of the following administrative states: ERX system, destination, tunnel, and session. This setting, rather than the administrative state of the session, determines whether the ERX system can maintain this session or not.
 - State – status of the session: idle, connecting, established, or disconnecting
 - Local and peer session id – names the ERX system uses to identify the session locally and remotely
 - › Statistics – information about the traffic for this session
 - › Session operational configuration – information received from the peer when the session was created

- Example 1

```

host1#show l2tp session
L2TP session 1/1/1 is Up
1 L2TP session found

```

- Example 2

```

host1#show l2tp session detail
L2TP session 1/1/1 is Up
Configuration
Administrative state is enabled
SNMP traps are enabled

```

```

Session status
  Effective administrative state is enabled
  State is established
  Local session id is 25959, peer session id is 2
Statistics packets octets discards errors
Data rx 7      237    1      0
Data tx 6      160    0      0

```

```

Session operational configuration
  User name is 't1.s1@local'
  Tunneling PPP interface atm 0/0.1
  Call type is lacIncoming
  Call serial number is 0
  Bearer type is none
  Framing type is none
  Proxy LCP was provided
  Authentication method was chap

```

show l2tp session summary

- Use to display a summary of the configured and operational status of all L2TP sessions.
- Field descriptions
 - › Administrative status:
 - enabled – no restrictions on the creation of sessions
 - disabled – ERX system disabled these sessions
 - › Operational status:
 - up – session is available
 - down – session is unavailable
 - lower-down – session is unavailable because the tunnel supporting it is inaccessible
 - not-present – session is unavailable because the hardware (such as a line module) supporting it is inaccessible
- Example

```

host1#show l2tp session summary
Administrative status  enabled    disabled
                    64          0

Operational
status      up        down    lower-down    not-present
           64          0         0             0

```

show l2tp tunnel

- Use to display detailed configuration information about specified tunnels.
- Field descriptions
 - › Configuration:
 - Administrative state – configured status of the tunnel
 - enabled – no restrictions on creation and operation of sessions for this tunnel
 - disabled – ERX system disabled existing sessions and will not create new sessions on this tunnel
 - drain – ERX system will not create new sessions on this tunnel

- SNMP traps – whether or not the ERX system sends traps to SNMP for operational state changes
- › Tunnel address:
 - Transport – method used to transfer traffic
 - Virtual router – name of the virtual router on which the tunnel is configured
 - Local and peer addresses – IP addresses of the local and remote ends of the tunnel
 - Local and peer UDP ports – UDP ports for the local and remote ends of the tunnel
- › Tunnel status:
 - Effective administrative state – most restrictive of the following administrative states: ERX system, destination, and tunnel. This setting, rather than the administrative state of the tunnel, determines whether the ERX system can create new sessions on a tunnel or whether the sessions on a tunnel are disabled or not.
 - State – status of the tunnel: idle, connecting, established, or disconnecting
 - Local and peer tunnel id – names the ERX system used to identify the tunnel locally and remotely
- › Subinterfaces:
 - total – number of sessions that the ERX system has created on this tunnel
 - active – number of operational sessions on the tunnel
 - failed – number of requests that did not reach an operational state
- › Statistics – information about the traffic sent and received
- › Control channel statistics:
 - Receive window size – number of packets that the peer can transmit without receiving an acknowledgment from the ERX system
 - Receive ZLB – the number of acknowledgments that the ERX system has received from the peer
 - Receive out-of-sequence – number of received control packets that were out of order
 - Receive out-of-window – number of packets that arrived at the ERX system outside the receiving window
 - Transmit window size – number of packets that the ERX system can transmit before receiving an acknowledgment from the peer
 - Transmit ZLB – number of acknowledgments that the ERX system has sent to the peer
 - Transmit queue depth – number of packets that the ERX system is waiting to send to the peer, plus the number of packets for which the peer has not yet acknowledged receipt
- › Tunnel operation configuration – information received from the peer when the tunnel was created

• Example 1

```
host1#show l2tp tunnel virtual router default ip 172.31.1.98
L2TP tunnel 1/xyz is Up with 13 active sessions
L2TP tunnel 1/aol.com is Up with 13 active sessions
L2TP tunnel 1/isp.com is Up with 13 active sessions
L2TP tunnel 1/msn.com is Up with 13 active sessions
L2TP tunnel 1/mv.com is Up with 12 active sessions
5 L2TP tunnels found
```

• Example 2

```
host1#show l2tp tunnel detail 1/xyz
L2TP tunnel 1/xyz is Up with 13 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Tunnel address
  Transport ipUdp
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
  Local UDP port 1701, peer UDP port 1701
Tunnel status
  Effective administrative state is enabled
  State is established
  Local tunnel id is 14529, peer tunnel id is 34
Sub-interfaces      total    active    failed
Sessions            13      13       0
Statistics          packets  octets    discards  errors
Control rx         14      683       0         0
Control tx         41      4666      0         0
Data rx            67900944 67900944  0         0
Data tx            67900944 67900944  0         0
Control channel statistics
  Receive window size = 4
  Receive ZLB = 17
  Receive out-of-sequence = 0
  Receive out-of-window = 0
  Transmit window size = 4
  Transmit ZLB = 12
  Transmit queue depth = 0
  Retransmissions = 8
Tunnel operational configuration
  Peer host name is 'Juniper-POS'
  Peer vendor name is 'XYZ, Inc.'
  Peer protocol version is 1.1
  Peer firmware revision is 0x1120
  Peer bearer capabilities are digital and analog
  Peer framing capabilities are sync and async
```

show l2tp tunnel summary

- Use to display a summary of the configured and operational status of all L2TP tunnels.
- Field descriptions
 - › Administrative status:
 - enabled – no restrictions on the creation and operation of sessions for this tunnel
 - drain – ERX system will not create new sessions for this tunnel
 - disabled – ERX system disabled existing sessions and will not create new sessions for this tunnel
 - › Operational status:
 - up – tunnel is available
 - down – tunnel is unavailable
 - lower-down – tunnel is unavailable because the destination supporting it is inaccessible
 - not-present – tunnel is unavailable because the hardware (such as a line module) supporting the tunnel is inaccessible
- Example

```
host1#show l2tp tunnel summary
Administrative status  enabled   drain   disabled
                       5         0       0

Operational
status    up       down   lower-down   not-present
          5         0       0             0
```

