Chapter 11

L2TP Overview

Layer 2 Tunneling Protocol (L2TP) is a client-server protocol that allows Point-to-Point Protocol (PPP) to be tunneled across a network. This chapter includes the following topics that provide information for configuring L2TP on the E-series router.

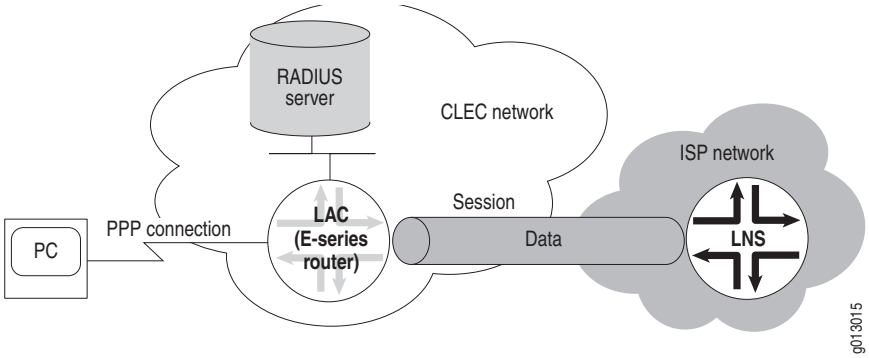
Overview

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 E-series router, receives packets from a remote client and forwards them to an L2TP network server (LNS), on a remote network.

You can configure your router 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.

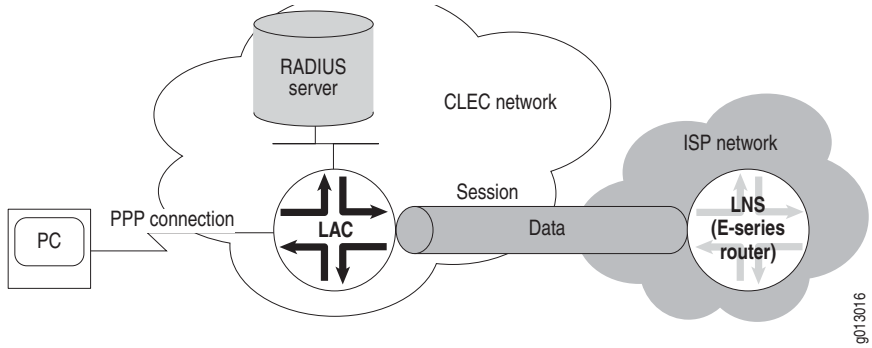
The E-series router creates tunnels dynamically by using authentication, authorization, and accounting (AAA) authentication parameters and transmits L2TP packets to the LNS via IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*. A tunnel is an aggregation of one or more sessions. Figure 7 and Figure 8 show the E-series router in typical LAC and LNS arrangements.

Figure 7: Using the E-series Router as an LAC



.

Figure 8: Using the E-series Router as an LNS



NOTE: The E-series router does not support terminating both ends of a tunnel or session in the same router.

L2TP Terminology

Table 65 describes the basic terms for L2TP.

Table 65: L2TP Terms

Term	Description
Attribute value pair (AVP)	Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
LAC	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.
LNS	L2TP network server (LNS)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. An LNS is the logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.

Table 65: L2TP Terms (continued)

Term	Description
Peer	In the L2TP context, refers to either the LAC or LNS. An LAC's peer is an LNS, and vice versa.
Proxy authentication	Authentication data from the PPP client that is sent from the LNS as part of a proxy LCP. Data might include attributes such as authentication type, authentication name, and authentication challenge.
Proxy LCP	LCP (Link Control Protocol) negotiation that is performed by the LAC on behalf of the LNS. Proxy sent by the LAC to the LNS containing attributes such as the last configuration attributes sent and received from the client.
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:** There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.
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 E-series router uses four levels:

- System—The router
- Destination—The remote L2TP system
- Tunnel—A direct path between the LAC and the LNS
- Session—A PPP connection in a tunnel

When the router 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 E-series router creates destinations, tunnels, and sessions dynamically, as follows:

1. The client initiates a PPP connection with the router.
2. The router and the client exchange Link Control Protocol (LCP) packets. For details about negotiating PPP connections, see *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol*.
3. By using either a local database related to the domain name or RADIUS authentication, the router determines either to terminate or to tunnel the PPP connection.

4. If the router 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 router 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 router discards received packets if the size of the variable-length, optional offset pad field in the L2TP header is too large. The router 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 E-series router sets up an LNS as follows:

1. An LAC initiates a tunnel with the router.

2. The router verifies that a tunnel with this LAC is valid—destination configured, hostname and tunnel password correct.

3. The router completes the tunnel setup with the LAC.

4. The LAC sets up a session with the router.

5. The router creates a dynamic PPP interface on top of the session.

6. If they are enabled and present, the router takes the proxy LCP and the proxy authentication data and passes them to PPP.

7. The E-series PPP processes the proxy LCP, if it is present, and, if acceptable, places LCP on the router in opened state without renegotiation of LCP.

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

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

9. The router passes the authentication results to the remote system.

Packet Fragmentation

The E-series router supports the reassembly of IP-fragmented L2TP packets. (For more information, see *JUNOSe IP Services Configuration Guide, Chapter 12, IP Reassembly for Tunnels*.) 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, you can configure the PPP MRU size by using the **ppp mru** command in Profile Configuration mode, Interface Configuration mode, or Subinterface Configuration mode. Use Profile Configuration mode for dynamic PPP interfaces, and Interface Configuration mode or Subinterface Configuration mode for static PPP interfaces.

When you specify the size, you need to take into account the MRU for all possible links between the LAC and the LNS. You 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 applies:

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

If the smallest intervening link is an Ethernet link, specifying **ppp mru 1442** at either the LAC or LNS guarantees that no fragmentation will occur within the L2TP tunnel.

Platform Considerations

For information about modules that support LNS and LAC on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

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

For information about modules that support LNS and LAC on the E120 router and the E320 router:

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

Module Requirements

The supported modules for LNS depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

To use an LNS on ERX-7xx models, ERX-14xx models, and the ERX-310 router, at least one Service line module (SM) or a module that supports the use of shared tunnel-server ports must be installed in the ERX router. For information about installing modules in the ERX router, see the *ERX Hardware Guide*.

SMs provide dedicated tunnel-server ports that are always configured on the module. Unlike other line modules, SMs do not pair with corresponding I/O modules that contain ingress and egress ports. Instead, they receive data from and transmit data to other line modules with access to ingress and egress ports on their own associated I/O modules.

You can also create tunnels on E-series modules that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services. For a list of the modules that support shared tunnel-server ports, see the *ERX Module Guide*.

For information about configuring tunnel services on dedicated and shared tunnel-server ports, see *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

For information about line modules supported by the LAC and LNS and the type of support each module type receives, see *ERX Module Guide, Appendix A, Module Protocol Support*.

E120 Router and E320 Router

To use an LNS on an E120 router or an E320 router, you must install an ES2 4G line module (LM) with an ES2-S1 Service I/O adapter (IOA), or an IOA that supports the use of shared tunnel-server ports. For information about installing modules in these routers, see the *E120 and E320 Hardware Guide*.

The ES2 4G LM and ES2-S1 Service IOA combination provides a dedicated tunnel-server port that is always configured on the IOA. Unlike SMs, the ES2 4G LM requires the ES2-S1 Service IOA to condition it to receive and transmit data to other line modules. The ES2-S1 Service IOA also does not have ingress or egress ports.

You can also create tunnels on IOAs that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the IOA's bandwidth to provide tunnel services. For a list of the IOAs that support shared tunnel-server ports, see the *E120 and E320 Module Guide*.

For information about IOAs supported by the LAC and LNS and the type of support each module type receives, see *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Sessions and Tunnels Supported

The E120 and E320 routers support 60,000 L2TP sessions, the ERX-1440 router supports 32,000 L2TP sessions, and all other E-series routers support a maximum of 16,000 L2TP sessions. The following guidelines apply:

- On all E-series routers

  The SM and the ES2-S1 Service IOA both support the termination of 16,000 LNS sessions per module. Therefore, if you want to apply input or output policies to all of the available LNS sessions, you can only terminate a maximum of 8000 sessions per module.

- On the E120 router, E320 router, and the ERX-1440 router

  You can create a systemwide maximum of 60,000 sessions per E120 or E320 router or 32,000 sessions per ERX-1440 router. The maximum session limit is spread in any combination across a maximum of 8000 tunnels. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and the router's applicable maximum sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

- On all E-series routers except the ERX-1440 router, E120 router, and the E320 router

You can create a systemwide maximum of 16,000 sessions spread in any combination across a maximum of 8000 tunnels shared between an LAC and an LNS. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and 16,000 sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

NOTE: In previous releases, the JUNOSe software required that you use the **license l2tp-session** command to configure a license to enable support for the maximum allowable L2TP sessions on ERX-1440 routers, E120 routers, and E320 routers. The **license l2tp-session** command still appears in the CLI, but it has no effect on the actual enforced limit. The reported license limit is 60,000. The **show license l2tp-session** command also still appears in the CLI.

- To obtain the maximum number of ingress and egress policy attachments supported for L2TP sessions, see *JUNOSe Release Notes, Appendix A, System Maximums*.

References

For more information about L2TP, see the following resources:

- RFC 2661—Layer Two Tunneling Protocol "L2TP" (August 1999)
- RFC 3145—L2TP Disconnect Cause Information (July 2001)
- Fail Over extensions for L2TP "failover"—draft-ietf-l2tpext-failover-06.txt (April 2006 expiration)

For information about L2TP high availability support, see *JUNOSe System Basics Configuration Guide, Chapter 7, Managing High Availability*.

For information about setting up policy-based routing features for L2TP, such as rate limit profiles, classifier control lists, and policy lists, see the *JUNOSe Policy Management Configuration Guide*.

For information about creating and attaching QoS profiles to L2TP sessions, see the *JUNOSe Quality of Service Configuration Guide*.

For information about how to secure Layer 2 Tunneling Protocol (L2TP) tunnels with IP Security (IPSec) on your E-series router, see *JUNOSe IP Services Configuration Guide, Chapter 13, Securing L2TP and IP Tunnels with IPSec*.