Chapter 14

Configuring L2TP Dial-Out

This chapter describes the Layer 2 Tunneling Protocol (L2TP) dial-out feature on your E-series router. This chapter includes the following sections:

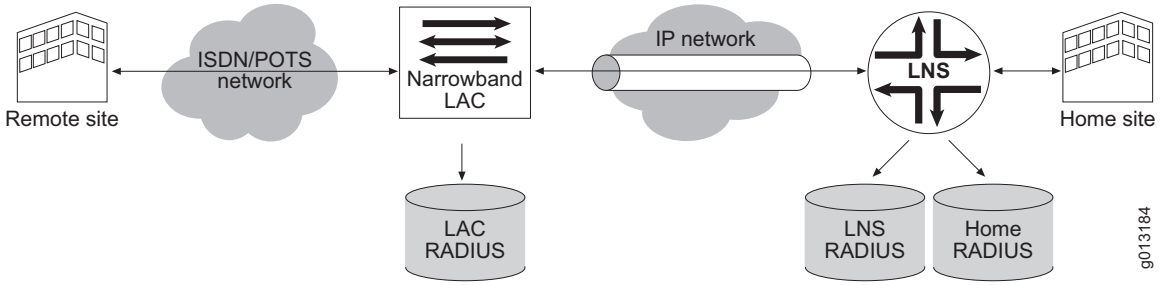
Overview

L2TP dial-out provides a way for corporate virtual private networks (VPNs) that use Broadband Remote Access Server (B-RAS) to dial out to remote offices that have only narrowband dial-up access. The L2TP network server (LNS) function is deployed in networks that have a combination of broadband and narrowband access.

A remote site can communicate on demand with the home site with a normal L2TP access concentrator (LAC) to LNS session. When the communication finishes, the remote site terminates the session. However, if the home site wishes to communicate with the remote site and no incoming call is currently established, the home site needs a method to dial out to the remote site. This method is L2TP dial-out, which uses the L2TP outgoing call support defined in RFC 2661—Layer Two Tunneling Protocol “L2TP” (August 1999).

Figure 10 shows the dial-out model in which the LNS initiates L2TP sessions and provides enough information to the narrowband LAC so that it can complete the dial-out from the home site to the remote site.

Figure 10: Network Model for Dial-Out



NOTE: The dial-out feature exists in the LNS only. It does not exist in the LAC.

Terms

Table 47 describes key terms used in L2TP dial-out.

Table 47: L2TP Dial-Out Terms

Term	Description
Dial-out trigger	IP packet that initiates a dial-out session
Dial-out session	Control entity for a triggered IP flow used to manage the establishment of an associated L2TP session for dial-out
Dial-out target	A virtual router context and an IP address prefix, for which the arrival of an IP packet (a dial-out trigger) initiates a dial-out session.
Dial-out route	Contains the dial-out target, as well as a domain name and profile. ■ The domain name is used in the initial Access-Request message. ■ The profile is used to create the IP/Point-to-Point Protocol (PPP) stack for the dial-out session.

Network Model for Dial-Out

In Figure 10, the home site connects to the Internet over a permanent leased line to the Internet service provider's (ISP's) E-series LNS. The ISP uses an IP network to connect the LNS to the narrowband access point of the network where the narrowband LAC exists. The narrowband LAC connects to a narrowband network (ISDN) that the remote site is also connected to.

The figure shows three RADIUS servers. The home site maintains the home server, and the other two servers are at the LNS and the LAC. The router accesses the home and LNS RADIUS servers. (The separation of the RADIUS servers is transparent to the router.)

Before any attempts at connectivity can take place from the home site to the remote site, an administrator must configure a dial-out route on the router. This route directs the router to start a dial-out operation. The route includes a dial-out target (the virtual router context and the IP address of the remote site). When the router receives a packet destined for the target, it triggers a dial-out session to the target. The route is associated with a profile that holds parameters for the interface stack that the router builds as a result of the dial-out.

Dial-Out Process

The following is the dial-out process used in the Figure 10 network:

1. The router receives a trigger packet.

2. The router builds a RADIUS Access-Request message and sends it to the RADIUS server that is associated with the virtual router on which the dial-out route is defined—typically, the RADIUS home server.

3. The RADIUS server's response to the Access-Request is similar to the response used for LAC incoming calls. Notable differences are that the IP addresses of the peer are interpreted as LAC addresses instead of LNS addresses. In addition, narrowband details, such as calling numbers, are returned.

4. The LNS makes the outgoing call using a load-balancing or round-robin mechanism identical to the one that the E-series LAC uses for incoming calls. The LAC may also employ the LAC RADIUS in tunnel authentication.

5. Once the LNS successfully completes a control connection and session with the LAC, the LAC performs the actual narrowband dial-out operation to the remote site using the information passed by the LNS during session setup.

6. A PPP session is started on the remote customer premises equipment (CPE), and mutual PPP authentication is performed at the remote CPE and the LNS as follows:

    a. The LNS uses the LNS RADIUS server to validate the remote CPE's PPP session, while the CPE can use its own RADIUS server to validate the LNS's PPP session.

    b. The LNS uses the username and password that is returned in the first Access-Accept message.

7. Once authentication is successful, an IP interface is built on top of the PPP interface at the LNS. Internet Protocol Control Protocol (IPCP) is negotiated, and the framed route that RADIUS returns as a result of the PPP authentication supersedes the dial-out route.

IP traffic can now flow freely between the home and remote sites.

Dial-Out Operational States

The dial-out state machine is a control process within the router that manages the dial-out function for each IP flow. The dial-out state machine has four levels of control: the router chassis, virtual router, targets, and sessions. This section describes the operational states of each of these levels.

Chassis

Table 48 describes the operational states of the chassis.

Table 48: Chassis Operational States

State	Description
inService	Dial-out service is operational at the chassis level.
initializationFailed	Dial-out service could not obtain enough system resources for basic operation. All configuration commands fail, and the dial-out service does not function.

Virtual Router

Table 49 describes the operational states of the virtual router.

Table 49: Virtual Router Operational States

State	Description
inService	Dial-out service is operational for the virtual router.
initPending	Dial-out service is waiting for the virtual router to be operational. Targets defined within the virtual router are not functional.
down	The dial-out interface for this virtual router is down. Targets defined within the virtual router are not functional.

Targets

Table 50 describes the operational states of the targets.

Table 50: Target Operational States

State	Description
inService	Dial-out route is up and operational.
inhibited	Dial-out service cannot obtain sufficient resources to handle triggers, and all triggers are discarded. When resources become available, a target can transition from inhibited to inService. Note that sessions within an inhibited target that are already in the process of connecting or are in the inService state are not affected by this condition.
down	There are insufficient resources to support the creation of a dial-out route for the target. When resources become available, the target can transition to inService. Note that sessions within a down target that are already in the process of connecting or are in the inService state are not affected by this condition.

Sessions

Table 51 describes operational states of the sessions.

Table 51: Session Operational States

State	Description
authenticating	New sessions start in the authenticating state. In this state, the dial-out state machine has received a valid trigger and is waiting for authentication, authorization, and accounting (AAA) to complete the initial authentication. On getting a grant from AAA, the session transitions to the connecting state. Alternatively, on getting a deny from AAA, the session transitions to the inhibited state.
connecting	Sessions enter the connecting state when authentication is complete. In this state, the dial-out state machine has initiated an outgoing L2TP call. On entering this state, the session-connecting timer is set to the chassis-wide trigger timer value. The session stays in this state until either the outgoing call is successful or the connecting timer expires. Any new trigger packets received for this session when it is in the connecting state are discarded.
inService	A session enters the inService state from the connecting state on successful completion of the dial-out call request. The session stays in this state until the outgoing call is closed.
inhibited	A session enters the inhibited state from the connecting state when the connecting timer expires (that is, the outgoing call was unsuccessful). This state prevents the router from thrashing on an outgoing call that cannot be completed. When in this state, the router discards all trigger packets received for the session. The inhibited timer controls the amount of time spent in this state. The setting of the inhibited timer varies depending on whether the session is entering the inhibited state for the first time or is reentering the state. ■ If it is the first time, the inhibited timer is initialized to the chassis-wide trigger value. ■ If it is reentering the state, the inhibited timer is initialized to 2 times the previous value of the inhibited timer, up to a maximum of 8 times the chassis-wide trigger value. For example, if the chassis-wide trigger value is 30 seconds, the setting of the inhibited timer within the session (on subsequent immediate reentries; see postInhibited state) is 30, 60, 120, 240. Since 240 is 8 x 30, the inhibited timer for this session is never set larger than 240 seconds.
postInhibited	A session enters the postInhibited state after completion of an inhibited state. The inhibited timer is reused to control the amount of time the session stays in postInhibited state. In this state the timer repeatedly times out and reduces the inhibited timer by a factor of 2 on each iteration. Once the inhibited timer reaches zero, the session transitions to dormant. The receipt of a trigger in this state results in a transition to the authenticating state.
dormant	A session enters the dormant state after completion of a postInhibited state. The dormant timer is initialized to the chassis-wide dormant timer value, minus the time the session spent in the postInhibited state. Receipt of a new trigger packet transitions the session to the authenticating state. If the dormant timer expires, the session is deleted. The dormant state exists to allow analysis of a dial-out session before it is deleted.

Table 51: Session Operational States (continued)

State	Description
pending	A session enters the pending state when a valid trigger is received but there already are the maximum number of connecting sessions in the router. The router discards all subsequent trigger packets until other sessions transition out of the connecting state. When this happens, pending sessions can transition to the dormant state.
failed	A session enters the failed state when the router detects a configuration error that prevents the successful operation of the session. Specifically, one of the final steps in a dial-out request is mutual PPP authentication at the LNS. A side-effect of authentication is the installation of an access route for the outgoing call. If the access route does not correspond to the trigger packet (that is, the trigger packet cannot be routed successfully by the new access route), the router detects this discrepancy as a configuration error because trigger packets that arrive are not forwarded into the outgoing call; rather, they are buffered or discarded. The only way to exit the failed state is with the **l2tp dial-out session reset** command.

Outgoing Call Setup Details

This section details the process described in *Dial-Out Process* on page 335.

Access-Request Message

To create the username in the authentication request, the router uses the trigger, dial-out route, domain name, and optional Multiprotocol Label Switching (MPLS) route distinguisher (RD). The username is constructed as follows:

[MPLS RD]/{trigger destination address}@domain-name

For example, given a dial-out route with an IP prefix of 10.10.0.0/16, a domain name of L2TP-dial-out.de.dt, and an MPLS RD of 0.0.0.0:65000, if a trigger packet arrives with a destination IP address of 10.10.1.1, the router creates the following username:

0.0.0.0:65000/10.10.1.1@L2TP-dial-out.de.dt

No password is offered, and the authentication request is passed to the S-series AAA server for normal authentication processing.

Using the above example, the AAA domain map processes the L2TP-dial-out.de.dt domain as for any other domain. If RADIUS authentication is configured for the authenticating virtual router (VR) context, AAA passes the authentication request to the E-series RADIUS client. The RADIUS authentication request is consistent with other requests, except that the Service-Type attribute is set to outbound (value of 5).

Access-Accept Message

The router expects RADIUS attributes that define a tunnel to be returned with the additions in Table 52. If tunnel attributes are excluded from the Access-Accept message or the returned Service-Type attribute is not set to outbound, the dial-out session is denied.

Table 52: Additions to RADIUS Attributes in Access-Accept Messages

Attribute Number	Attribute Name	Content
6	Service-Type	Outbound
67	Tunnel-Server-Endpoint	IP address of LAC
Juniper VSA 26-35	Tunnel-Dialout-Number	L2TP dial-out number
Juniper VSA 26-36	PPP-Username	Username used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-37	PPP-Password	Password used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-38	PPP-Protocol	Authentication protocol used for L2TP sessions. 0 = none 1 = PAP 2 = CHAP 3 = PAP-CHAP 4 = CHAP-PAP
Juniper VSA 26-39	Tunnel-Min-Bps	Minimum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-40	Tunnel-Max-Bps	Maximum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-41	Tunnel-Bearer-Type	Bearer capability required: 0 = name; 1 = analog; 2 = digital. Passed to LAC (not interpreted by the LNS).

Outgoing Call

After receiving a valid tunnel definition from AAA, the E-series LNS initiates an outgoing call. The router follows the same load-sharing mechanisms as for incoming calls. See *Configuring LAC Tunnel Selection Parameters* in ***Chapter 12, Configuring an L2TP LAC***.

After an outgoing call is successfully signaled, the router dynamically creates a PPP interface. The profile in the dial-out route definition specifies any PPP configuration options. Both the L2TP session and the PPP interface exist on a Tunnel Service module, identical to the LNS operation for incoming calls.

Once the PPP interface is created, Link Control Protocol (LCP) and IPCP are negotiated.

Mutual Authentication

Mutual authentication takes place in LCP, where the LNS validates the PPP interface on the remote CPE and vice-versa. LNS takes the same actions to authenticate the peer as it does on incoming calls.

The LNS obtains the PPP username and password from the initial Access-Accept message. It then provides this information to the remote CPE for authentication.

Route Installation

Once authentication is complete, the router creates a new access route. This route directs the forwarding of IP packets related to the original trigger packet to the newly created interface. The route does not need to be identical to the one specified in the dial-out route, but it must be able to forward packets that have the same destination address as the trigger packet. However, if the access route does not encompass the dial-out route definition, any other trigger packets initiate a new dial-out session.

The dial-out state machine verifies that the trigger packet can be forwarded over the route.

- If the verification is unsuccessful, the dial-out session is put into the failed state.
- If the verification is successful, the dial-out session is put into the inService state.

Platform Considerations

L2TP dial-out is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about L2TP, see RFC 2661—Layer Two Tunneling Protocol "L2TP" (August 1999).

Before You Configure L2TP Dial-Out

Create a profile that the router uses to create the dynamic PPP and IP interfaces on the LNS. The profile specifies parameters that are common to all dial-out sessions that use the profile. The following is an example of a typical profile configuration.

1. Create a profile.

   host1(config)#**profile dialOut**
   host1(config-profile)#

2. Specify the interface used for dialout.

   host1(config-profile)#**ip unnumbered loopback 0/0**

3. Specify the virtual router for the dial-out user's IP interface.

   host1(config-profile)#**ip virtual-router lns**

4. Specify the authentication mechanism.

   host1(config-profile)#**ppp authentication chap**

Configuring L2TP Dial-Out

To configure L2TP dial-out:

1. Enable the creation of a dial-out session.

   host1(config)#**l2tp dial-out target 10.10.0.0 255.255.0.0 L2TP-dial-out.de.dt profile dialOut**

2. (Optional) Set the maximum time allowed for successful establishment of an L2TP dial-out session.

   host1(config)#**l2tp dial-out connecting-timer-value 30**

3. (Optional) Set how long the dial-out session stays in the dormant state waiting for a new trigger after the associated L2TP outgoing call ends.

   host1(config)#**l2tp dial-out dormant-timer-value 300**

4. (Optional) Set the maximum number of trigger packets held in buffer while the dial-out session is being established.

   host1(config)#**l2tp dial-out max-buffered-triggers 50**

You can also:

- Manually delete a dial-out session.

  host1#**l2tp dial-out session delete 10.10.0.0**

- Reset a dial-out session by forcing it to the dormant state.

  host1#**l2tp dial-out session reset 10.10.0.0**

l2tp dial-out connecting-timer-value

- Use to set the maximum time allowed for attempts to establish L2TP dial-out sessions.
- If the session fails to be established before the connecting timer expires, subsequent attempts to establish the dial-out session to the same destination are inhibited temporarily.
- The range is 30–3600 seconds.
- Example

  host1(config)#**l2tp dial-out connecting-timer-value 30**

- Use the **no** version to set the connecting timer to the default, 30 seconds.

l2tp dial-out dormant-timer-value

- Use to set how long the dial-out session waits in the dormant state for a new trigger after the associated L2TP outgoing call ends.
- If no trigger is received before the dormant timer expires, the dial-out session is deleted.
- The range is 0–3600 seconds.
- Example

  host1(config)#**l2tp dial-out dormant-timer-value 300**

- Use the **no** version to set the dormant timer to the default, 300 seconds (5 minutes).

l2tp dial-out max-buffered-triggers

- Use to set the maximum number of buffered trigger packets held for any dial-out session pending the successful establishment of the L2TP session. Once the session is established, the buffered trigger packets are transmitted.
- Trigger packets received when the maximum number of triggers are already buffered are discarded.
- The range of values is 0–50.
- Example

  host1(config)#**l2tp dial-out max-buffered-triggers 50**

- Use the **no** version to set the number of trigger buffers to the default, 0.

l2tp dial-out session delete

- Use to delete a dial-out session.
- Closes any L2TP outgoing call associated with the dial-out session.
- Example

  host1#**l2tp dial-out session delete 10.10.0.0**

- There is no **no** version.

l2tp dial-out session reset

- Use to force the dial-out session to the dormant state where it remains until the dormant timer expires or it receives a new trigger.
- Closes any L2TP outgoing call associated with the dial-out session.
- Example

  host1#**l2tp dial-out session reset 10.10.0.0**

- There is no **no** version.

l2tp dial-out target

- Use to define an L2TP dial-out target. When the router receives packets destined for the target, it creates a dial-out session.
- When you create a target, you must specify the following:
  - *ipAddress*—IP address of the target
  - *ipAddressMask*—IP address mask of the target
  - *domainName*—Domain name used in the outgoing call Access-Request message
  - *profileName*—Name of profile used to create the interface stack
- Example

  host1(config)#**l2tp dial-out target 10.10.0.0 255.255.0.0 L2TP-dial-out.de.dt profile dialOut**

- Use the **default** version to remove the L2TP dial-out route.
- Use the **no** version to remove the L2TP dial-out route or target.

Monitoring L2TP Dial-Out

To monitor L2TP dial-out, see:

- Monitoring Chassis-wide Configuration for L2TP Dial-out on page 368
- Monitoring Status of Dial-out Sessions on page 372
- Monitoring Dial-out Targets within the Current VR Context on page 373
- Monitoring Operational Status within the Current VR Context on page 374