Chapter 12

Configuring an L2TP LAC

An L2TP access concentrator (LAC) receives packets from a remote client and forwards them to an L2TP network server (LNS), on a remote network. You can configure your E-series router to function as an LAC.

This chapter includes the following topics that provide information for configuring an L2TP LAC on the E-series router:

LAC Configuration Prerequisites

Before you begin configuring the router as a LAC, perform the following steps:

1. Create a virtual router.

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

2. Assign a router ID IP address, such as that for a loopback interface, to the virtual router. This address must be reachable by the L2TP peer.

   host1:west(config)#**ip router-id 10.10.45.3**

CAUTION: You must explicitly assign a router ID to a virtual router rather than using a dynamically assigned router ID. A fixed ID is required because every time the ID changes, L2TP must disconnect all existing tunnels and sessions that use the old ID. If you use a dynamically assigned router ID, the value can change without warning, leading to failure of all L2TP tunnels and sessions. Also, the router could dynamically assign a router ID that is not reachable by the L2TP peer, causing a complete failure of L2TP. You must set the router ID even if you specified a source address in the domain map or a local address in the host profile.

3. When configuring the router as a LAC, configure the router or virtual router for Broadband Remote Access Server (B-RAS).

NOTE: If you are using shared tunnel-server ports, you must configure the shared tunnel-server ports before you configure Layer 2 Tunneling Protocol (L2TP) network server (LNS) support. You use the **tunnel-server** command in Global Configuration mode to specify the physical location of the shared tunnel-server port that you want to configure.

See *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces* for additional information about the **tunnel-server** command and shared tunnel-server ports.

Related Topics

- **virtual-router** command
- **ip router-id** command

Modifying L2TP LAC Default Settings for Managing Destinations, Tunnels, and Sessions

Configuring an E-series router for B-RAS enables the router to operate as an LAC with default settings. You can modify the default settings as follows:

- Enable the verification of data integrity via UDP.
- Specify the time period for which the router maintains dynamic destinations, tunnels, or sessions after termination.

NOTE: The previous two operations also apply to an LNS, however there is no default configuration that enables the LNS.

When the router 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.
- Configure drain timeout operations, which control the amount of time a disconnected LAC tunnel waits before restarting after receiving a restart request.
- Configure how many times the router retries a transmission if the initial attempt is unsuccessful.

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

Related Topics

- Generating UDP Checksums in Packets to L2TP Peers on page 274
- Specifying a Destruct Timeout for L2TP Tunnels and Sessions on page 274
- Preventing Creation of New Destinations, Tunnels, and Sessions on page 275
- Shutting Down Destinations, Tunnels, and Sessions on page 276
- Specifying the Number of Retransmission Attempts on page 278

Generating UDP Checksums in Packets to L2TP Peers

You can configure the router to generate a UDP data integrity checksum in data packets sent to an L2TP peer. The router always uses UDP checksums during transmission and reception of L2TP control packets. Generation of checksums is disabled by default.

- To enable generation of UDP checksums:

  host1(config)#**l2tp checksum**

This command does not affect the way the router checks the UDP data integrity checksum in L2TP data packets that are received from an L2TP peer. The router checks all non-zero received checksums and discards the packet if a data integrity problem is detected.

Related Topics

- **l2tp checksum** command

Specifying a Destruct Timeout for L2TP Tunnels and Sessions

You can specify the maximum time period, in the range 10–3600 seconds (1 hour), for which the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed. The router uses a timeout of 600 seconds by default.

This command facilitates debugging and other analysis by saving underlying memory structures after the destination, tunnel, or session is terminated.

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.

TIP: If you use the **l2tp destination lockout timeout** command to configure an optional lockout timeout, always configure the destruct timeout to be longer than the lockout timeout. The destruct timeout overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the lockout timeout and lockout test settings. See *Managing the L2TP Destination Lockout Process* on page 290.

- To specify a destruct timeout:

  host1(config)#**l2tp destruct-timeout 1200**

Related Topics

- **l2tp destruct-timeout** command

Preventing Creation of New Destinations, Tunnels, and Sessions

You can configure several L2TP drain operations, which determine how the router creates new L2TP destinations, tunnels, and sessions. You can manage the following features:

- Prevent creation of new destinations, tunnels, and sessions on the router
- Prevent creation of new tunnels and sessions at a specific destination
- Prevent creation of new sessions for a specific tunnel
- Specify how long a disconnected LAC L2TP tunnel waits before restarting after it receives a restart request

Preventing Creation of New Destinations, Tunnels, and Sessions on the Router

You use the **l2tp drain** command to prevent the creation of new destinations, tunnels, and sessions on the router.

The **l2tp drain** command and the **l2tp shutdown** command both affect the administrative state of L2TP on the router. 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.

- To prevent the creation of new destinations, tunnels, and sessions:

  host1(config)#**l2tp drain**

Preventing Creation of New Tunnels and Sessions at a Destination

You use the **l2tp drain destination** command to prevent the creation of new tunnels and sessions at a specific destination.

The **l2tp drain destination** 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.

- To prevent the creation of new tunnels and sessions at the specified destination:

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

Preventing Creation of New Sessions for a Tunnel

Use the **l2tp drain tunnel** command to prevent the creation of new sessions for a tunnel.

The **l2tp drain tunnel** 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.

- To prevent the creation of new sessions for a specific tunnel:

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

Preventing Creation of New Sessions for a Tunnel

Use the **l2tp tunnel short-drain-timeout** command to specify the amount of time a disconnected LAC L2TP tunnel waits before restarting after it receives a restart request.

You can specify a drain timeout in the range 0–31 seconds. This feature enables the router to restart tunnels more quickly than the standard 31-second drain time specified by RFC-2661. By default, the router uses a short-drain timeout of 2 seconds.

- To specify the short-drain timeout:

  host1(config)#**l2tp tunnel short-drain-timeout 12**

Related Topics

- **l2tp drain** command
- **l2tp drain destination** command
- **l2tp drain tunnel** command
- **l2tp tunnel short-drain-timeout** command

Shutting Down Destinations, Tunnels, and Sessions

You can configure how the router shuts down L2TP destinations, tunnels, and sessions. You can specify the following shut down methods, which also prevent the creation of new tunnels:

- Close all destinations, tunnels, and sessions on the router and prevent creation of new destinations, tunnels, and sessions
- Close all tunnels and sessions, and prevent creation of new tunnels and sessions, at a specific destination
- Close all sessions and prevent creation of new sessions for a specific tunnel
- Close a specific session

Closing Existing and Preventing New Destinations, Tunnels, and Sessions on the Router

You use the **l2tp shutdown** command to close all existing destinations, tunnels, and sessions, and to prevent the creation of new destinations, tunnels, and sessions on the router.

The **l2tp shutdown** command and the **l2tp drain** command both affect the administrative state of L2TP on the router. 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.

- To close all destinations, tunnels, and sessions on the router:

  host1(config)#**l2tp shutdown**

Closing Existing and Preventing New Tunnels and Sessions for a Destination

You use the **l2tp shutdown destination** command to close all existing tunnels and sessions for a destination and to prevent the creation of tunnels and sessions for that destination.

The **l2tp shutdown destination** 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.

- To close tunnels and sessions, and prevent creation of new tunnels and sessions for the specified destination:

  host1(config)#**l2tp shutdown destination 1**

Closing Existing and Preventing New Sessions in a Specific Tunnel

You use the **l2tp shutdown tunnel** command to close all sessions in a tunnel and to prevent the creation of sessions in a tunnel.

The **l2tp shutdown tunnel** 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.

- To close all existing sessions in a specific tunnel and prevent creation of new sessions:

  host1(config)#**l2tp shutdown tunnel 1/isp.com**

Closing a Specific Session

You use the **l2tp shutdown session** command to close the specified session.

- To close a specific session:

  host1(config)#**l2tp shutdown session 1/1/1**

Related Topics

- **l2tp shutdown** command
- **l2tp shutdown destination** command
- **l2tp shutdown session** command
- **l2tp shutdown tunnel** command

Specifying the Number of Retransmission Attempts

You can specify the number of retransmission attempts the router uses for tunnels, in the range 2–7. By default, the router uses a retry count of 5.

Use the **established** keyword to apply the retry count only to established tunnels. Use the **not-established** keyword to apply the retry count only to tunnels that are not established. If you do not include a keyword, the router applies the retry count to both established and nonestablished tunnels.

- To configure the number of retransmission attempts:

  host1(config)#**l2tp retransmission 4 established**

Related Topics

- **l2tp retransmission** command

Configuring Calling Number AVP Formats

The E-series LAC generates L2TP Calling Number AVP 22 for incoming-call request (ICRQ) packets that the LAC sends to the LNS. By default, the E-series LAC generates the Calling Number AVP 22 in descriptive format.

You can also prevent the E-series LAC from sending the Calling Number AVP in ICRQ packets.

NOTE: You cannot change the L2TP Calling Number AVP on tunnel switched interfaces.

You use the **aaa tunnel calling-number-format** command to configure the router to generate AVP 22 in any of the following formats. Agent-circuit-id is suboption 1 of the tags supplied by the PPPoE intermediate agent from the DSLAM. Agent-remote-id is suboption 2.

- Descriptive format—This is the default format, and includes the following elements:

  < interface ID > < delimit > < UID > < delimit > < interface description > < delimit > < connect info > < delimit > < PPPoE description >

- Descriptive include-agent-circuit-id format—This format includes the following elements:

  < interface ID > < delimit > < UID > < delimit > < interface description > < delimit > < connect info > < delimit > < PPPoE description > < delimit > < agent-circuit-id >

- Descriptive include-agent-circuit-id include-agent-remote-id format—This format includes the following elements:

  < interface ID > < delimit > < UID > < delimit > < interface description > < delimit > < connect info > < delimit > < PPPoE description > < delimit > < agent-circuit-id > < delimit > < agent-remote-id >

- Descriptive include-agent-remote-id format—This format includes the following elements:

  < interface ID > < delimit > < UID > < delimit > < interface description > < delimit > < connect info > < delimit > < PPPoE description > < delimit > < agent-remote-id >

- Fixed format—This format is similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id). If you set up the router to generate the Calling Number AVP in fixed format, the router formats the AVP as follows (the maximum number of characters for each field is shown in brackets):

  - For ATM: < system name [4] > < slot [2] > < port [1] > < VPI [3] > < VCI [5] >

  - For Ethernet: < system name [4] > < slot [2] > < port [1] > < VLAN [8] >

  - Example

    system name = westford, slot = 4, port = 3, and VLAN = 12 produces the following calling number:

    west0430000000012

- Include-agent-circuit-id format—This format includes the following element:

  < agent-circuit-id >

- Include-agent-circuit-id include-agent-remote-id format—This format includes the following elements:

  < agent-circuit-id > < delimit > < agent-remote-id >

- Include-agent-remote-id format—This format includes the following element:

  < agent-remote-id >

Configuration Tasks

To set up the router to generate Calling Number AVP 22 in fixed format:

1. Set the calling number format of the tunnel to **fixed**.

   host1(config)#**aaa tunnel calling-number-format fixed**

2. Set the format of the RADIUS Calling-Station-Id to **fixed**.

   host1(config)#**radius calling-station-format fixed-format**

Configuring the Fallback Format

You can configure a fallback AVP 22 format—the E-series LAC uses the fallback format to generate the L2TP Calling Number AVP 22 in the event that the PPPoE agent ID is null or unavailable. The LAC uses the fallback format only when the configured calling number format includes either or both of the agent-circuit-id and agent-remote-id suboptions. You can specify either descriptive format or fixed format.

The calling number format determines what element triggers use of the fallback format, as shown in the following table:

Calling Number Format	Fallback Trigger
agent-circuit-id	agent-circuit-id is empty
agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
agent-remote-id	agent-remote-id is empty
descriptive include-agent-circuit-id	agent-circuit-id is empty
descriptive include-agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
descriptive include-agent-remote-id	agent-remote-id is empty

- To configure the fallback AVP format:

  host1(config)#**aaa tunnel calling-number-format-fallback fixed**

Disabling the Calling Number AVP

You can use the **l2tp disable calling-number-avp** command to prevent the E-series LAC from sending the Calling Number AVP in ICRQ packets. You use this command in special situations where you do not want the LAC to send this AVP.

- To prevent the LAC from sending the Calling Number AVP:

  host1(config)#**l2tp disable calling-number-avp**

For more information about setting up the router to generate Calling Number AVP 22 in a format that includes either or both of the agent-circuit-id and agent-remote-id suboptions of the tags supplied by the PPPoE intermediate agent, see *Configuring PPPoE Remote Circuit ID Capture* in *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*.

Configuration Examples

The following examples show how you can synchronize the contents of RADIUS Calling-Station-Id (Attribute 31) and L2TP Calling-Number (AVP 22).

To send the PPPoE agent-circuit-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when the PPPoE agent-circuit-id is unavailable, issue the following commands:

host1(config)#**radius calling-station-format fixed-format**
host1(config)#**radius remote-circuit-id-delimiter #**
host1(config)#**radius override calling-station-id remote-circuit-id**
host1(config)#**radius remote-circuit-id-format agent-circuit-id**

host1(config)#**aaa tunnel calling-number-format include-agent-circuit-id**
host1(config)#**aaa tunnel calling-number-format-fallback fixed**

To send the PPPoE agent-circuit-id and agent-remote-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when both PPPoE agent-circuit-id and agent-remote-id are unavailable, issue the following commands:

host1(config)#**radius calling-station-format fixed-format**
host1(config)#**radius remote-circuit-id-delimiter #**
host1(config)#**radius override calling-station-id remote-circuit-id**
host1(config)#**radius remote-circuit-id-format agent-circuit-id agent-remote-id**

host1(config)#**aaa tunnel calling-number-format include-agent-circuit-id include-agent-remote-id**
host1(config)#**aaa tunnel calling-number-format-fallback fixed**

Related Topics

- **aaa tunnel calling-number-format** command
- **aaa tunnel calling-number-format-fallback** command
- **l2tp disable calling-number-avp** command
- **radius calling-station-format** command

Mapping a User Domain Name to an L2TP Tunnel Overview

The router uses either the local database related to the domain name or a RADIUS server to determine whether to terminate or tunnel PPP connections.

For information about setting up RADIUS to provide this mapping, see *Chapter 1, Configuring Remote Access*.

For a given domain map, you can choose one of two methods to map the domain to an L2TP tunnel locally on the router:

- Configure tunnels for a domain map and then define tunnel attributes from Domain Map Tunnel configuration mode.
- Configure a tunnel group and then define the attributes for its tunnels from Tunnel Group Tunnel Configuration mode. Use this method only when no tunnels are currently defined for the domain map from Domain Map Tunnel configuration mode. By default, tunnel groups are not assigned to the domain map.

  After configuring a tunnel group and the attributes for its tunnels, you can assign the tunnel group to the domain map from Domain Map mode. The tunnel group reference in the domain map is used instead of tunnel definitions configured from Domain Map Tunnel configuration mode.

  The RADIUS server can reference tunnel groups through the RADIUS Tunnel Group [26-64] attribute. The advantages of RADIUS support for tunnel groups are:

  - The RADIUS server can maintain a single tunnel group attribute associated with each user instead of sets of tunnel attributes for each user.
  - The RADIUS server can authenticate users before attempting to establish tunnels.

Related Topics

- Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 282
- Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 286

Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Domain Map Tunnel mode, perform the following steps:

1. Specify a domain name and enter Domain Map Configuration mode:

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

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

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

3. Specify a tunnel to configure and enter Domain Map Tunnel Configuration mode:

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

4. Specify the LNS endpoint address of a tunnel.

   host1(config-domain-map-tunnel)#**address 192.0.2.13**

5. (Optional) Assign a tunnel group to the domain map. You can assign a tunnel group only when no tunnels are currently defined for the domain map from AAA Domain Map Tunnel mode.

   host1(config-domain-map)#**tunnel group storm**

6. Specify a preference for the tunnel.

   You can specify up to eight levels of preference, and you can assign the same preference to a maximum of 31 tunnels. When you define multiple preferences for a destination, you increase the probability of a successful connection.

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

7. (Optional) Specify an authentication password for the tunnel.

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

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

8. (Optional) Specify a hostname for the LAC end of the tunnel.

   The LAC sends the hostname to the LNS when communicating to the LNS about the tunnel. The hostname can be up to 64 characters (no spaces).

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

NOTE: If the LNS does not accept tunnels from unknown hosts, and if no hostname is specified, the LAC uses the router name as the hostname.

9. (Optional) Specify a server name for the LNS.

   This name specifies the hostname 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 (no spaces).

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

10. (Optional) Specify a source IP address for the LAC tunnel endpoint. All L2TP packets sent to the peer use this source address.

    host1(config-domain-map-tunnel)#**source-address 192.0.3.3**

By default, the router uses the virtual router's router ID as the source address. You can override this behavior for an L2TP tunnel by specifying a source address. If you do specify a source address, use the address of a stable IP interface (for example, a loopback interface). Make sure that the address is configured in the virtual router for this domain map, and that the address is reachable by the peer.

11. Specify a tunnel identification. (The router groups L2TP sessions with the same tunnel identification into the same tunnel.)

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

    The router groups L2TP sessions with the same tunnel identification into the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.

12. Specify the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type). Currently, the only supported value is L2TP.

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

13. Specify a medium type for the tunnel. (L2TP supports only IP version 4 [IPv4].)

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

14. (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**

    If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name.

15. (Optional) Specify a default tunnel password.

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

    If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password.

16. (Optional) Set the format for the tunnel assignment ID that is passed to PPP/L2TP.

    The tunnel assignment ID format can be either only assignmentID or clientAuthId + serverAuthId + assignmentId.

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

    If you do not set a tunnel assignment ID, the software sets it to the default (assignmentID). This parameter is only generated and used by the L2TP LAC device.

17. (Optional) Specify whether or not to use the tunnel peer's Nas-Port [5] and Nas-Port-Type [61] attributes.

    When enabled, the attribute is supplied by the tunnel peer. When disabled, the attribute is not supplied. Use the **no** version of the command to restore the default, enable.

    ```
    host1(config)#aaa tunnel ignore nas-port enable
    host1(config)#aaa tunnel ignore nas-port-type disable
    ```

18. (Optional) Set up the router to ignore sequence numbers in data packets received on L2TP tunnels.

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

    This command does not affect the insertion of sequence numbers in packets *sent* from the router.

BEST PRACTICE: We recommend that you set up the router to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly might reorder L2TP packets, out-of-order packets might be dropped when sequence numbers are being used on L2TP data packets.

---

19. (Optional) Disable the generation of authentication challenges by the local tunnel, so that the tunnel does not send a challenge during negotiation. However, the tunnel does accept and respond to challenges it receives from the peer.

    ```
    host1(config)#l2tp disable challenge
    ```

20. Verify the L2TP tunnel configuration.

```
host1(config)#show aaa domain-map

Domain: westford.com; router-name: default; ipv6-router-name: default
                                                                    Tunnel
Tunnel   Tunnel         Tunnel        Tunnel   Tunnel    Tunnel    Tunnel   Client
 Tag      Peer          Source         Type    Medium   Password     Id      Name
------   ------------   -----------   ------   ------   ---------  ------   ------
3        192.168.2.13   192.168.3.3   l2tp     ipv4     temporary  acton    host4

         Tunnel                Tunnel                      Tunnel
Tunnel   Server     Tunnel       Max                       Virtual
 Tag      Name    Preference   Sessions     Tunnel RWS     Router
------   ------   ----------   --------   --------------   -------
3        boston   5            0          system chooses   vr2

                            host1#show aaa tunnel-parameters
                            Tunnel password is 3&92k%b#q4
                            Tunnel client-name is <NULL>
                            Tunnel nas-port-method is none
                            Tunnel nas-port ignore disabled
                            Tunnel nas-port-type ignore disabled
                            Tunnel assignmentId format is assignmentId
                            Tunnel calling number format is descriptive
```

Related Topics

- Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 286
- **aaa domain-map** command
- **aaa tunnel assignment-id-format** command
- **aaa tunnel client-name** command
- **aaa tunnel ignore** command
- **aaa tunnel password** command
- **address** command
- **client-name** command
- **identification** command
- **l2tp disable challenge** command
- **l2tp ignore-receive-data-sequencing** command
- **medium ipv4** command
- **password** command
- **preference** command
- **router-name** command
- **server-name** command
- **source-address** command
- **tunnel** command
- **tunnel group** command
- **type** command

Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Tunnel Group Tunnel Configuration mode, perform the following steps:

1. Specify an AAA tunnel group and change the mode to Tunnel Group Tunnel Configuration mode. From Tunnel Group Tunnel Configuration mode, you can add up to 31 tunnel definitions.

   ```
   host1(config)#aaa tunnel-group westford
   host1(config-tunnel-group)#
   ```

2. Specify a tunnel to configure and enter Tunnel Group Tunnel Configuration mode:

   host1(config-tunnel-group)#**tunnel 3**
   host1(config-tunnel-group-tunnel)#

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

   host1(config-tunnel-group-tunnel)#**router-name default**

4. Specify the LNS endpoint address of a tunnel.

   host1(config-tunnel-group-tunnel)#**address 192.0.2.13**

5. Specify a preference for the tunnel.

   You can specify up to eight levels of preference, and you can assign the same preference to a maximum of 31 tunnels. When you define multiple preferences for a destination, you increase the probability of a successful connection.

   host1(config-tunnel-group-tunnel)#**preference 5**

6. (Optional) Specify an authentication password for the tunnel.

   host1(config-tunnel-group-tunnel)#**password temporary**

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

7. (Optional) Specify a hostname for the LAC end of the tunnel.

   The LAC sends the hostname to the LNS when communicating to the LNS about the tunnel. The hostname can be up to 64 characters (no spaces).

   host1(config-tunnel-group-tunnel)#**client-name host4.**

NOTE: If the LNS does not accept tunnels from unknown hosts, and if no hostname is specified, the LAC uses the router name as the hostname.

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

   This name specifies the hostname 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 (no spaces).

   host1(config-tunnel-group-tunnel)#**server-name boston**

9. (Optional) Specify a source IP address for the LAC tunnel endpoint. All L2TP packets sent to the peer use this source address.

   By default, the router uses the virtual router's router ID as the source address. You can override this behavior for an L2TP tunnel by specifying a source address. If you do specify a source address, use the address of a stable IP interface (for example, a loopback interface). Make sure that the address is configured in the virtual router for this domain map, and that the address is reachable by the peer.

   host1(config-tunnel-group-tunnel)#**source-address 192.0.3.3**

10. Specify a tunnel identification.

    host1(config-tunnel-group-tunnel)#**identification acton**

    The router groups L2TP sessions with the same tunnel identification into the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.

11. Specify a medium type for the tunnel. (L2TP supports only IP version 4 [IPv4].)

    host1(config-tunnel-group-tunnel)#**medium ipv4**

12. Specify the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type). Currently, the only supported value is L2TP.

    host1(config-tunnel-group-tunnel)#**type l2tp**

13. Verify the L2TP tunnel configuration.

```
host1(config)#show aaa domain-map

Domain: westford.com; router-name: default; ipv6-router-name: default
                                                                    Tunnel
Tunnel   Tunnel         Tunnel        Tunnel   Tunnel    Tunnel    Tunnel   Client
 Tag      Peer           Source        Type    Medium   Password     Id      Name
------   ------------   -----------   ------   ------   ---------  ------   ------
3        192.168.2.13   192.168.3.3   l2tp     ipv4     temporary  acton    host4

         Tunnel                Tunnel                      Tunnel
Tunnel   Server     Tunnel       Max                        Virtual
 Tag      Name    Preference   Sessions     Tunnel RWS      Router
------   ------   ----------   --------   --------------   -------
3        boston   5            0          system chooses   vr2
```

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
tunnel assignmentId format is assignmentId
aaa tunnel calling number format is descriptive
```

Related Topics

- Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 282
- **aaa tunnel-group** command
- **address** command
- **client-name** command
- **identification** command
- **medium ipv4** command
- **password** command
- **preference** command
- **router-name** command
- **server-name** command
- **source-address** command
- **tunnel** command
- **type** command

Configuring the RX Speed on the LAC

You can configure the E-series LAC to always generate L2TP Receive (RX) Speed AVP 38. If you do not specify this command, the RX Speed AVP is generated only when the RX speed differs from the TX speed. The AVPs can be used to generate the RADIUS Connect-Info attribute [77] on the LNS.

To set up the router to always generate the Receive Speed (AVP 38), complete the following steps:

1. On the ATM subinterface, configure the advisory receive speed. See *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM* for information about configuring the advisory speed.

   host1(config-subif)#**atm atm1483 advisory-rx-speed 2000**

2. Specify that the RX Speed AVP is always generated. If you do not specify this command, the RX Speed AVP is generated only when the RX speed differs from the TX speed.

   host1(config)#**l2tp rx-connect-speed-when-equal**

Related Topics

- **atm atm1483 advisory-rx-speed** command
- **l2tp rx-connect-speed-when-equal** command

Managing the L2TP Destination Lockout Process

When multiple sets of tunneling parameters are available, L2TP uses a selection algorithm to choose the best tunnel for subscriber traffic. As part of this selection process, the JUNOSe software's L2TP implementation includes a lockout feature in which the router locks out, or disregards, destinations that are assumed to be unavailable.

By default, when a destination becomes unavailable, L2TP locks out that destination for a lockout timeout of 300 seconds (5 minutes). After the lockout timeout expires, L2TP assumes that the destination is now available and includes the destination when performing the selection algorithm.

Modifying the Lockout Procedure

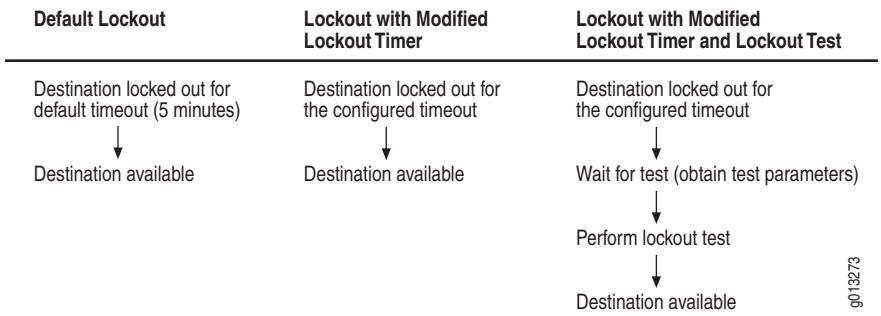
You can optionally configure your own lockout procedure by specifying the lockout timeout you want to use or enabling a lockout test, or both. When the lockout timeout expires, the destination is either immediately unlocked (if lockout testing is not enabled) or begins the lockout test to verify that the destination is available.

L2TP performs the lockout test by attempting to establish a tunnel to the unavailable destination. For the test, L2TP must first obtain the parameters for a tunnel to the destination. If no such tunnel currently exists, L2TP must wait until it receives a new session request that has tunnel parameters for the locked out destination. The destination remains locked out while L2TP waits for the tunnel parameters and becomes available only after successful completion of the lockout test. Therefore, if lockout testing is enabled, the destination is actually locked out longer than the lockout timer you specify.

NOTE: Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described in **Specifying a Destruct Timeout for L2TP Tunnels and Sessions** on page 274) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service. As a result, the locked out destination might be returned to service prior to expiration of your configured lockout timeout and without completion of the lockout test you specified.

Figure 9 shows how locked-out destinations transition from a locked-out state to available status when using the default lockout configuration, a configuration that includes a modified lockout timer, and a configuration with both a modified timer and the lockout test.

Figure 9: Lockout States



You can use the following commands to manage L2TP destination lockout and configure a lockout process that meets the needs of your network environment:

- Use the **l2tp destination lockout-timeout** command to modify the default lockout timeout period.
- Use the **l2tp destination lockout-test** command to configure L2TP to perform a lockout test, which verifies that a currently locked out destination is now available and to include it in the selection algorithm.
- Use the **l2tp unlock destination** command to force L2TP to immediately unlock the specified locked out destination; the destination is then considered to be available by the selection algorithm. L2TP disregards any time remaining in the existing lockout timeout and also disregards the lockout test (if configured).
- Use the **l2tp unlock-test destination** command to force L2TP to immediately begin the lockout testing procedure for the specified destination; any time remaining in the existing lockout timeout is not taken into account.
- Use the **show l2tp** and **show l2tp destination lockout** commands to view information about the L2TP configuration and statistics.

Verifying that a Locked-Out Destination is Available

You can use the **l2tp destination lockout-test** command to configure L2TP to test locked-out destinations; this verifies that a previously locked-out destination is available before the router changes the destination's status.

- To verify the availability of locked out destinations:

  host1(config)#**l2tp destination lockout-test**

Configuring a Lockout Timeout

You use the **l2tp destination lockout-timeout** command to configure the amount of time (in seconds) between when an L2TP destination is found to be unavailable and when it is eligible for unlocking. When the timeout period expires, L2TP either begins the lockout test procedure (if configured to do so) or immediately returns the destination to available state.

BEST PRACTICE: Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described in **Specifying a Destruct Timeout for L2TP Tunnels and Sessions** on page 274) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service.

You can specify a lockout timeout in the range 60–3600 seconds (1 minute–1 hour). The router uses a timeout value of 300 seconds by default.

- To configure an L2TP lockout timeout:

  host1(config)#**l2tp destination lockout-timeout 500**

  The new lockout timeout only affects future locked-out destinations; it does not affect destinations that are currently locked out.

Unlocking a Destination that is Currently Locked Out

You use the **l2tp unlock destination** command to force L2TP to immediately unlock the specified L2TP destination, which is currently locked out and unavailable. L2TP then considers the destination to be available. Any remaining lockout time and the lockout test setting (if configured) are not taken into account.

You must be at privilege level 10 or higher to use this command.

- To unlock a currently locked-out destination:

  host1(config)#**l2tp unlock destination ip 192.168.1.98**

Starting an Immediate Lockout Test

You use the **l2tp unlock-test destination** command to force L2TP to immediately start the lockout test for the specified destination—any remaining lockout time for the destination is ignored.

You must be at privilege level 10 or higher to use this command.

NOTE: If lockout testing is not configured, this command immediately unlocks the destination and L2TP then considers the destination to be available

---

- To force an immediate lockout test for a specific destination:

  host1(config)#**l2tp unlock-test destination ip 192.169.110.8**

Related Topics

- **l2tp destination lockout-timeout** command
- **l2tp destination lockout-test** command
- **l2tp unlock destination** command
- **l2tp unlock-test destination** command

Managing Address Changes Received from Remote Endpoints

A remote endpoint can use the Start-Control-Connection-Reply (SCCRP) packets that it sends to the E-series LAC to change the address that the LAC uses to communicate with the endpoint. By default, the LAC accepts the change and uses the new address to communicate with the endpoint. However, you can configure the LAC to ignore or reject the requested change. Setting up the LAC to ignore address changes in SCCRP packets enables the router to construct tunnels with separate receive and transmit addresses and to avoid problems due to a misconfiguration. Three possible configurations are available:

- Default configuration—The E-series LAC accepts the change from the endpoint. The LAC then sends all subsequent packets to, and accepts packets from, the new address.
- Ignore configuration (specified by the **l2tp ignore-transmit-address-change** command)—The LAC continues to send packets to the original address but accepts packets from the new address.

  host1(config)#**l2tp ignore-transmit-address-change**

  Use the **ip-address** or **udp-port** keyword to ignore the specific address component. Omit the keywords to ignore the entire address change in the SCCRP packet.
- Reject configuration (specified by the **l2tp reject-transmit-address-change** command)—The LAC sends a Stop-Control-Connection-Notification (StopCCN) to the original address, then terminates the connection to the endpoint.

  host1(config)#**l2tp reject-transmit-address-change ip-address**

  Use the **ip-address** or **udp-port** keyword to reject the specific address component. Omit the keywords to reject the entire address change in the SCCRP packet.

The reject specification takes precedence over the ignore specification.

The router accepts a change in receive address only once, during the tunnel establishment phase, and only on an SCCRP packet. Subsequent changes result in the router dropping packets. Any changes do not affect established tunnels.

Use the **show l2tp** command to display the SCCRP address change configuration.

Related Topics

- **l2tp ignore-transmit-address-change** command
- **l2tp reject-transmit-address-change** command

Configuring LAC Tunnel Selection Parameters

This section presents the capabilities of the LAC's tunnel selection process. L2TP allows you to specify:

- Up to 31 destinations for a domain.
- Up to eight levels of preference. Preference indicates the order in which the router attempts to connect to the destinations specified for a domain. Zero (0) is the highest level of preference.
- Up to 31 destinations for a single preference level.

For information about setting up destinations and preference levels for a domain, see *Mapping a User Domain Name to an L2TP Tunnel Overview* on page 281.

When the E-series LAC determines that a PPP session should be tunneled, it selects a tunnel from a set of tunnels associated with either the PPP user or the PPP user's domain. The router provides the following methods for selecting tunnels:

- Tunnel selection failover between preference levels (the default behavior)
- Tunnel selection failover within a preference level
- Maximum sessions per tunnel
- Weighted load balancing

Configuring the Failover Between Preference Levels Method

When a user tries to log into a domain, in the default method, the router attempts to connect to a destination in that domain with the highest preference level. If more than one destination in the preference level is considered reachable, the router randomly selects a destination and attempts to contact it. If the router is unsuccessful, it marks the destination as unreachable and does not try to connect to that destination for five minutes. The router then moves to the next lower preference level and repeats the process. The router makes up to eight attempts to connect to a destination for a domain—one attempt for each preference level.

If all destinations at a preference level are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. The key is to understand that the router 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.

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 a PPP user tries to connect to the domain, suppose the router randomly selects destination A from preference 0. If this connection attempt fails, the router 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 router excludes destination B, as well as destination A, and attempts to connect to destination C, the only destination available with preference 2. The router 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 Overview* on page 281.

- To enable tunnel selection failover between preference levels:

  This tunnel selection method is the default method. If you do not set any tunnel selection parameters, the router uses this method.

Configuring the Failover Within a Preference Level Method

You use the **l2tp fail-over-within-preference** command to enable tunnel selection failover within a preference level.In this selection method, if the router tries to connect to a destination and is unsuccessful, it selects a new destination at the same preference level. If all destinations at a preference level are marked as unreachable, the router does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

If all destinations at all preference levels are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. If the connection fails, the router rejects the PPP user session without attempting to contact the remote router.

For example, suppose there are four tunnels for a domain: A, B, C, and D. All tunnels are considered reachable, and the preference levels are assigned as follows:

- A and B at preference 0
- C and D at preference 1

When the router attempts to connect to the domain, suppose it randomly selects tunnel B from preference 0. If it fails to connect to tunnel B, the router excludes tunnel B for five minutes and attempts to connect to tunnel A. If this attempt also fails, the router drops to preference 1. Then suppose the router selects tunnel C. If it also fails to connect to tunnel C, the router excludes tunnel C for five minutes and attempts to connect to tunnel D.

- To enable tunnel selection failover within a preference level:

  host1(config)#**l2tp fail-over-within-preference**

Configuring the Maximum Sessions per Tunnel

You can configure the maximum number of sessions per tunnel, either through a RADIUS server or the command-line interface. If you set the maximum sessions per tunnel parameter, the router takes the setting into consideration when it selects a tunnel. If a randomly selected tunnel has a current session count equal to its maximum session count, the router does not attempt to contact that tunnel. Instead, it makes an alternate tunnel selection from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the router drops to the next lower preference level to make the next selection. This process is consistent, regardless of which fail-over scheme is currently running on the router. A tunnel without a configured maximum sessions value has no upper limit on the number of sessions it can support.

The router uses a default value of 0 (zero), which allows unlimited sessions in the tunnel.

- To configure the maximum sessions per tunnel.

  host1(config)#**aaa domain-map lac0ne**
  host1(config-domain-map)#**tunnel 1**
  host1(config-domain-map-tunnel)#**max-sessions 1500**

Configuring the Weighted Load Balancing Method

With the weighted load-balancing method, the router uses the maximum sessions per tunnel to choose among multiple tunnels that share the same preference level.

The weight of a tunnel is proportional 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. The router uses a round-robin tunnel selection method by default.

- To configure the router to base tunnel selection within a preference level on the maximum sessions per tunnel.

  host1(config)#**l2tp weighted-load-balancing**

Related Topics

- **l2tp fail-over-within-preference** command
- **l2tp weighted-load-balancing** command
- **max-sessions** command