Chapter 13

Configuring an L2TP LNS

An L2TP network server (LNS) is 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. You can configure your E-series router to function as an LNS.

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

LNS Configuration Prerequisites

Before you begin configuring the router as an LNS, 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.

Related Topics

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

Configuring an 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 router, the UDP port used for L2TP traffic is closed, and no tunnels or sessions can be established.

To enable an LAC to connect to the LNS, you must create the following profiles:

- An L2TP destination profile—Defines the location of each LAC
- An L2TP host profile—Defines the attributes used when communicating with an LAC

NOTE: If you remove a destination profile or modify attributes of a host profile, all tunnels and sessions using the profile will be dropped.

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.

To configure an LNS, perform the following steps:

1. Create a destination profile that defines the location of the LAC, and access L2TP Destination Profile Configuration mode. See *Creating an L2TP Destination Profile* on page 315.

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

2. Define the L2TP host profile and enter L2TP Destination Profile Host Configuration mode. See *Creating an L2TP Host Profile* on page 315.

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

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

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

4. (Optional) Disable the use of proxy LCP when connecting to the selected host.

   ```
   host1(config-l2tp-dest-profile-host)#disable proxy lcp
   ```

5. (Optional) Enable the use of proxy authentication when connecting to the selected host.

   ```
   host1(config-l2tp-dest-profile-host)#enable proxy authenticate
   ```

6. (Optional) Specify the local hostname to be used in any hostname AVP sends to the LAC. By default, the router name is used as the local hostname.

   ```
   host1(config-l2tp-dest-profile-host)#local host andy
   ```

7. (Optional) Specify the local IP address to be used in any packets sent to the LAC. By default, the router ID is used.

   ```
   host1(config-l2tp-dest-profile-host)#local ip address 192.168.23.1
   ```

8. (Optional) Specify the shared secret used to authenticate the tunnel. By default, there is no tunnel authentication.

   ```
   host1:boston(config-l2tp-dest-profile-host)#tunnel password saco
   ```

9. (Optional) Specify that L2TP create an MLPPP interface when LCP proxy data is not forwarded from the LAC.

   For example, the MLPPP interface is created if the LAC does not send the initial received or last received LCP configuration request. If full LCP proxy data is available, this command is ignored.

   host1:boston(config-l2tp-dest-profile-host)#**default-upper-type mlppp**

NOTE: When acting as the LNS, the E-series router supports dialed number identification service (DNIS). With DNIS, if users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing. See *Using DNIS* in *Chapter 1, Configuring Remote Access*.

Related Topics

- Creating an L2TP Destination Profile on page 315
- Creating an L2TP Host Profile on page 315
- Configuring the Maximum Number of LNS Sessions on page 316
- Configuring the RADIUS Connect-Info Attribute on the LNS on page 317
- Selecting Tunnel-Service Modules for LNS Sessions Using MLPPP on page 317
- **bundled-group-id** command
- **bundled-group-id-overrides-mlppp-ed** command
- **default-upper-type mlppp** command
- **disable proxy lcp** command
- **enable proxy authenticate** command
- **l2tp destination profile** command
- **local host** command
- **local ip address** command
- **max-sessions** command
- **radius connect-info-format** command
- **remote host** command
- **tunnel password** command

Creating an L2TP Destination Profile

You use the **l2tp destination profile** command to create the destination profile that defines the location of the LAC, and to access L2TP Destination Profile Configuration mode.

If no virtual router is specified with the command, 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.

- To create a destination profile:

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

NOTE: When you change an L2TP destination profile, you must wait for the router to delete all L2TP tunnels associated with the deleted profile before you create the new profile.

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

Related Topics

- Creating an L2TP Host Profile on page 315
- **remote host** command

Creating an L2TP Host Profile

Use the **remote host** command to define the L2TP host profile and access L2TP Destination Profile Host Configuration mode.

- 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 you specify any name other than *default* for the remote host, then the LAC must supply the specified hostname in order for the tunnel to be set up. The remote hostname is matched against the hostname AVP in the received Start-Control-Connection-Request (SCCRQ).
- The remote hostname can be up to 64 characters (no spaces).

- Example

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

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

NOTE: If you modify any attributes of a host profile, all tunnels and sessions using that profile will be dropped.

Related Topics

- Creating an L2TP Destination Profile on page 315
- **l2tp destination profile** command

Configuring the Maximum Number of LNS Sessions

You can use the **max-sessions** command in both L2TP Destination Profile Configuration mode and L2TP Destination Profile Host Configuration mode to configure the number of sessions allowed by the L2TP network server (LNS).

The LNS uses a two-step process to ensure that the maximum number of allowed sessions is not exceeded. When a session is requested, the LNS first checks the maximum sessions set for the L2TP destination profile. If no limit is set, or if the current count is less than the configured limit, the LNS then performs the same check on the L2TP destination host profile limit. If the current count is also less than the L2TP destination host profile limit, then the new session can be established. If a session request exceeds either of the max-sessions settings, the LNS rejects the session.

NOTE: New sessions are rejected once the chassis-wide session limit is exceeded, even if the destination profile or host profile maximum session limit is not exceeded. For information about the maximum number of L2TP sessions supported per chassis, see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

- To set the maximum sessions allowed for the specified destination, use the **max-sessions** command in L2TP Destination Profile Configuration mode:

  host1(config)#**l2tp destination profile westford ip address 10.10.21.2**
  host1(config-l2tp-destination-profile)#**max-sessions 20000**

- To set the maximum session allowed for the specified host, use the **max-sessions** command in L2TP Destination Profile Host Configuration mode:

  host1(config-dest-profile))#**remote host default**
  host1(config-l2tp-destination-profile-host)#**max-sessions 20000**

Related Topics

- **max-sessions** command

Configuring the RADIUS Connect-Info Attribute on the LNS

You can configure the LNS to generate the RADIUS Connect-Info attribute [77]. Service providers can then use the information in the RADIUS attribute to identify a customer's service.

On the LNS, the Connect-Info attribute is based on the L2TP connect-speed AVPs received from the LAC. The LNS does not generate the attribute by default. The format of the Connect-Info attribute is as follows, where the TX speed and RX speed are equal to the respective L2TP AVPs:

```
tx-speed [ /rx-speed ]
```

The TX speed is always included in the attribute when the speed is not zero; however, inclusion of the RX speed depends on the keyword you use with the command.

- Use the **l2tp-connect-speed** keyword to specify that the RX speed is only included when it is not zero and also is different than the TX speed.

  ```
  host1(config)#radius connect-info-format l2tp-connect-speed
  ```

- Use the **l2tp-connect-speed-rx-when-equal** keyword to specify that the RX speed is always included when it is not zero.

  ```
  host1(config)#radius connect-info-format l2tp-connect-speed-rx-when-equal
  ```

Related Topics

- **radius connect-info-format** command

Selecting Tunnel-Service Modules for LNS Sessions Using MLPPP

You can install multiple tunnel-service modules in an E-series router deployed as an LNS where the tunnel sessions carry MLPPP. To use an LNS, at least one Service line module (SM), ES2-S1 Service IOA, or a module that supports the use of shared tunnel-server ports must be installed in the E-series router.

The router selects tunnel-service modules based on the LNS sessions that underlie the PPP link interfaces of an MLPPP bundle, also known as *bundled sessions*. To determine the appropriate SM where it places the first bundled session for an MLPPP bundle, the router uses a load-balancing mechanism. After the router determines the appropriate SM, it places all sessions for the same bundle on the same SM. By default, the router determines *bundled membership* based on the endpoint discriminator that the LNS receives from the LAC in the proxy LCP information.

For example, an ERX-1440 router has tunnel-service modules installed in slots 4, 9, and 12. Using the load-balancing mechanism, the router determines that the SM in slot 4 can accommodate the first bundled session for MLPPP bundle A, and places it there. The first bundled session for bundle A has an endpoint discriminator of 5. The router subsequently places all bundled sessions for bundle A (which have an endpoint discriminator of 5) on the SM in slot 4.

When the SM on which the bundled sessions reside has no more space for additional sessions, the router refuses the L2TP session. This can happen even when other tunnel-service modules installed in the router have available space.

For more information about endpoint discriminators, see *JUNOSe Link Layer Configuration Guide, Chapter 8, Configuring Multilink PPP*.

Assigning Bundled Group Identifiers

In some cases, an endpoint discriminator is not available for the LNS to use to identify the links in a bundled session.

This situation might occur when:

- PPP clients provide endpoint discriminators with null values.
- PPP clients do not provide an endpoint discriminator option when negotiating LCP with the LAC.
- The LAC does not include a endpoint discriminator option in the LCP proxy AVPs.

The router places all bundled sessions without endpoint discriminators on the same SM. However, if there are many such bundled sessions, the load-balanced distribution of LNS sessions across the tunnel-service modules can deteriorate because the router places all bundled sessions on the same SM without evenly distributing the load.

The **bundled-group-id** command enables you to correct this situation by assigning a numeric bundled group identifier for the router to use when the endpoint discriminator is unavailable to identify the bundled membership. The router places bundled sessions with the same bundled group identifier on the same SM in the same way that it does with endpoint discriminators.

The bundled group identifier applies to the entire router; therefore, if you assign the same bundled group identifier for different L2TP destination host profiles, the router places all of the bundled sessions with the same bundled group identifier on the same SM.

NOTE: We recommend that you assign bundled group identifiers only when you are certain that endpoint discriminators are unavailable to identify bundle membership.

- To assign a numeric bundled group identifier:

  host1:boston(config-l2tp-dest-profile-host)#**bundled-group-id 4**

Overriding All Endpoint Discriminators

NOTE: We strongly recommend that you use this feature only with the support of JTAC.

You can also configure the router to ignore the value of all endpoint discriminators when it selects a SM and to use only the bundled group identifier that you assigned by issuing the **bundled-group-overrides-mlppp-ed** command.

Issuing the **bundled-group-id** and **bundled-group-id-overrides-mlppp-ed** commands together forces the router to place the bundled sessions on the same SM when a PPP client incorrectly specifies different endpoint discriminators for links in the same bundle.

- To configure the router to ignore the value of all endpoint discriminators:

  host1:boston(config-l2tp-dest-profile-host)#**bundled-group-id-overrides-mlppp-ed**

Related Topics

- **bundled-group-id** command
- **bundled-group-id-overrides-mlppp-ed** command

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 there are two interface columns: one for the incoming session (LNS) and one for the outgoing session (LAC). The router forwards traffic from the incoming session to the outgoing session and vice versa.

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 E-series router.

- To enable tunnel switching:

  host1(config)#**l2tp tunnel-switching**

Related Topics

- **l2tp tunnel-switching** command

Creating Persistent Tunnels

The E-series router 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.

- To create a persistent tunnel, you configure an idle-timeout value of zero.

  host1(config)#**l2tp tunnel idle-timeout 0**

Related Topics

- **l2tp tunnel idle-timeout** command

Testing Tunnel Configuration

You can use the **l2tp tunnel test** command to force the establishment of a tunnel—this enables you to verify both the tunnel configuration and connectivity.

This command supports tunnel initiation: incoming calls on the LAC; outgoing calls on the LNS. The command does not support tunnel respondent: outgoing calls on the LAC; incoming calls on the LNS.

- To test a tunnel configuration:

  host1#**l2tp tunnel test portland.com gold**

Related Topics

- **l2tp tunnel test** command

Managing L2TP Destinations, Tunnels, and Sessions

When the router is established as an LNS you can manage the destinations, tunnels and sessions.

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

Related Topics

- *Generating UDP Checksums in Packets to L2TP Peers* in ***Chapter 12, Configuring an L2TP LAC***
- *Specifying a Destruct Timeout for L2TP Tunnels and Sessions* in ***Chapter 12, Configuring an L2TP LAC***
- *Preventing Creation of New Destinations, Tunnels, and Sessions* in ***Chapter 12, Configuring an L2TP LAC***
- *Shutting Down Destinations, Tunnels, and Sessions* in ***Chapter 12, Configuring an L2TP LAC***
- *Specifying the Number of Retransmission Attempts* in ***Chapter 12, Configuring an L2TP LAC***

Configuring Disconnect Cause Information

You can configure an E-series LNS to convey PPP-related disconnect cause information to its L2TP peer. Enabling an LNS to send disconnect cause information to an LAC is particularly useful in an environment where the LAC initiates tunnels without a client's request, knowledge, or approval. In this type of environment, all PPP signaling for the tunnel session takes place between the LNS and the client, without active participation of the LAC. As a result, the LAC is not aware of the reason that a session has disconnected.

NOTE: An E-series LAC does not send PPP Disconnect Case Code AVPs to an LNS. In the event that a third-party LAC does send the AVP to an E-series LNS, the LNS discards the AVP.

Generating the Disconnect Cause AVP Globally

You use the **l2tp disconnect-cause** command to specify that the LNS include the PPP Disconnect Cause Code AVP in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to the LAC. For example, this feature enables the LAC to obtain information about the cause of a session disconnection,

- To enable disconnect cause generation chassis-wide on the LNS:

  host1(config)#**l2tp disconnect-cause**

NOTE: Sessions for which the AVP generation is enabled by the host-profile-specific **disconnect-cause** command continue to generate the AVP.

Generating the Disconnect Cause AVP with a Host Profile

You use the **disconnect-cause** command in L2TP Destination Profile Host Configuration mode to specify that the E-series LNS generate PPP Disconnect Cause Code AVPs. This command pertains only to L2TP sessions to which the L2TP destination host profile applies. The AVP is included in all L2TP CDN messages that the LNS sends to an LAC for covered sessions.

NOTE: This command is used only for dial-in sessions; use the **l2tp disconnect-cause** command in Global Configuration mode to generate PPP Disconnect Cause Code AVPs for dial-out sessions.

- To enable disconnect cause generation for all tunnels that use a particular host profile on the LNS:

  host1(config-l2tp-dest-profile-host)#**disconnect-cause**

Enabling RADIUS Accounting for Disconnect Cause

You use the **radius include l2tp-ppp-disconnect-cause acct-stop enable** command to specify that the Disconnect-Cause RADIUS attribute (VSA 26-51) is generated and included in RADIUS acct-stop and acct-tunnel-link-stop records. RADIUS VSA 26-51 is not included in the accounting records by default.

At the LAC, this accounting reports remotely generated disconnect cause information received from the LNS. At the LNS, the accounting reports locally generated disconnect cause information.

- To enable disconnect cause accounting:

  host1(config)#**radius include l2tp-ppp-disconnect-cause acct-stop enable**

Displaying Disconnect Cause Statistics

You can display chassis-wide summary statistics for all disconnect cause information received by the LAC, sorted by code number.

- To display summary statistics for disconnect cause information:

  host1(config)#**show l2tp received-disconnect-cause-summary**

Related Topics

- **disconnect-cause** command
- **l2tp disconnect-cause** command
- **radius include l2tp-ppp-disconnect-cause acct-stop enable** command

Configuring the Receive Window Size

You can configure the L2TP receive window size (RWS) for an L2TP tunnel. L2TP uses the RWS to implement a sliding window mechanism for the transmission of control messages.

When you configure the RWS, you specify the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. If the RWS is not configured, the router determines the RWS and uses this value for all new tunnels on both the LAC and the LNS.

You can configure the L2TP RWS in the following ways:

- Configure the systemwide default RWS setting for a tunnel on both the LAC and the LNS by using the **l2tp tunnel default-receive-window** command (in Global Configuration mode).
- Configure the RWS for a tunnel on the LAC by using either the **receive-window** command (in Domain Map Tunnel Configuration mode) or by including the L2tp-Recv-Window-Size RADIUS attribute (VSA 26-54) in RADIUS Access-Accept messages.
- Configure the RWS for all tunnels that use a particular host profile on the LNS by using the **receive-window** command (in L2TP Destination Profile Host Configuration mode).

Configuring the Default Receive Window Size

Use the **l2tp tunnel default-receive-window** command to configure the default L2TP RWS for a tunnel on both the LAC and the LNS. The default L2TP RWS is the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. The only supported value is 4.

To configure the default RWS setting:

1. From Global Configuration mode, set the L2TP default RWS. The only value supported for the default RWS is 4.

   host1(config)#**l2tp tunnel default-receive-window 4**

   The router uses this RWS value for all new tunnels on both the LAC and the LNS. The new command has no effect on previously configured tunnels.

2. (Optional) Use the **show l2tp** command to verify the default RWS configuration.

```
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
  Retransmission retries for established tunnels is 5
  Retransmission retries for not-established tunnels is 5
  Tunnel idle timeout is 60 seconds
```

```
  Failover within a preference level is disabled
  Weighted load balancing is disabled
  Tunnel authentication challenge is enabled
  Calling number avp is enabled
  Ignore remote transmit address change is disabled
  Disconnect cause avp is disabled
  Default receive window size is 4
Sub-interfaces      total      active     failed     auth-errors
  Destinations      0          0          0          n/a
  Tunnels           0          0          0          0
  Sessions          0          0          0          n/a
  Switched-sessions 0          0          0          n/a
```

Configuring the Receive Window Size on the LAC

Use the **receive-window** command to configure the L2TP RWS for a tunnel on the LAC. Use the **no** version of the command to revert to the systemwide RWS setting configured with the **l2tp tunnel default-receive-window** command.

TIP: The RWS setting must be the same for all users of the same tunnel.

If you modify the RWS setting for an existing tunnel, subsequent tunnel users might be not be able to log in if their RWS setting conflicts with the new RWS setting for the tunnel.

To configure the RWS for a tunnel on the LAC:

1. Access Domain Map Tunnel Configuration mode as described in *Mapping a User Domain Name to an L2TP Tunnel Overview* in *Chapter 12, Configuring an L2TP LAC*. For example:

   ```
   host1(config)#aaa domain-map fms.com
   host1(config-domain-map)#router-name westford
   host1(config-domain-map)#tunnel 3
   host1(config-domain-map-tunnel)#
   ```

2. From Domain Map Tunnel Configuration mode, set the tunnel RWS. The only value supported for the tunnel RWS is 4, and it must be the same for all users of the same tunnel.

   ```
   host1(config-domain-map-tunnel)#receive-window 4
   ```

3. (Optional) Use the **show aaa domain-map** command to verify the RWS configuration.

   ```
   host1#show aaa domain-map

   Domain: fms.com; router-name: westford; ipv6-router-name: default
                                                                    Tunnel
   Tunnel   Tunnel   Tunnel   Tunnel   Tunnel    Tunnel    Tunnel   Client
    Tag      Peer    Source    Type    Medium   Password     Id      Name
   ------   ------   ------   ------   ------   --------   ------   ------
   3        <null>   <null>   l2tp     ipv4     <null>     <null>   <null>
            Tunnel                  Tunnel
   Tunnel   Server     Tunnel       Max      Tunnel
    Tag      Name    Preference   Sessions    RWS
   ------   ------   ----------   --------   ------
   ```

```
3        <null>   2000         0          4
```

You can also configure the RWS for a tunnel on the LAC by including the L2tp-Recv-Window-Size RADIUS attribute (VSA 26-54) in RADIUS Access-Accept messages. For more information about RADIUS Access-Accept messages, see *Chapter 3, Configuring RADIUS Attributes*. For more information about the L2tp-Recv-Window-Size attribute, see *Chapter 6, RADIUS Attribute Descriptions*.

Configuring the Receive Window Size on the LNS

Use the **receive-window** command to configure the L2TP RWS for a tunnel on the LNS. Use the **no** version of the command to revert to the systemwide RWS setting configured with the **l2tp tunnel default-receive-window** command.

To configure the RWS for a tunnel on the LNS:

1. Access L2TP Destination Profile Host Configuration mode. For example:

   host1(config)#**virtual-router fms02**
   host1:fms02(config)#**l2tp destination profile fms02 ip address 192.168.5.61**
   host1:fms02(config-l2tp-dest-profile)#**remote host fms03**
   host1:fms02(config-l2tp-dest-profile-host)#

2. From Destination Profile Host Configuration mode, set the tunnel RWS. The only value supported for the tunnel RWS is 4.

   host1:fms02(config-l2tp-dest-profile-host)#**receive-window 4**

TIP: If you modify the RWS setting of a host profile for an existing tunnel, the router drops the tunnel. This action is consistent with router behavior when you modify an L2TP host profile.

3. (Optional) Use the **show l2tp destination profile** command to verify the RWS configuration.

```
host1:fms02#show l2tp destination profile fms02
L2TP destination profile fms02
Destination address
  Transport ipUdp
  Virtual router fms02
  Peer address 192.168.5.61
Host profile attributes
  Remote host is fms03
    Receive window size is 4
1 L2TP host profile found
```

Related Topics

- **l2tp tunnel default-receive-window** command
- **receive-window** command

Configuring Peer Resynchronization

The JUNOSe software enables you to configure the peer resynchronization method you want the router to use. Peer resynchronization enables L2TP to recover from a router warm start and to allow an L2TP failed endpoint to resynchronize with its peer non-failed endpoint.

L2TP peer resynchronization:

- Prevents the non-failed endpoint from prematurely terminating a tunnel while the failed endpoint is recovering
- Reestablishes the sequence numbers required for the operation of the L2TP control protocol
- Resolves inconsistencies in the tunnel and session databases of the failed endpoint and the non-failed endpoint

To ensure successful peer resynchronization between endpoints, the non-failed endpoint must support a complete RFC-compliant L2TP implementation.

JUNOSe software supports both the L2TP silent failover method and the L2TP failover protocol method, which is described in Fail Over extensions for L2TP "failover" draft-ietf-l2tpext-failover-06.txt. You can configure L2TP to use the failover protocol method as the primary peer resynchronization method, but then fall back to the silent failover method if the peer does not support the failover protocol method.

The following list highlights differences between the failover protocol and silent failover peer resynchronization methods:

- With the L2TP failover protocol method, both endpoints must support the method or recovery always fails. The L2TP failover protocol method also requires a non-failed endpoint to wait an additional recovery time period while the failed endpoint is recovering to prevent the non-failed endpoint from prematurely disconnecting the tunnel. The additional recovery period makes L2TP less responsive to the loss of tunnel connectivity.
- Silent failover operates entirely within the failed endpoint and does not require non-failed endpoint support—this improves interoperability between peers. Silent failover does not require additional recovery time by the non-failed endpoint, which also eliminates the potential for degraded responsiveness to the loss of tunnel connectivity.

NOTE: L2TP silent failover is not supported on E3 ATM and CT1 line modules in peer-facing configurations.

You can use the CLI or RADIUS to configure the resynchronization method for your router.

Configuring Peer Resynchronization for L2TP Host Profiles and AAA Domain Map Tunnels

The JUNOSe CLI enables you to configure the peer resynchronization method globally, for a host profile, or for a domain map tunnel. A host profile or domain map tunnel configuration takes precedence over the global peer resynchronization configuration.

When you change the peer resynchronization method, the change is not immediately applied to existing tunnels. Tunnels continue using their current resynchronization method until the next time the tunnel is reestablished.

Use the **failover-resync** command to configure the L2TP peer resynchronization method for L2TP host profiles and AAA domain map tunnels. This command takes precedence over the global peer resynchronization configuration.

Choose one of the following keywords to specify the peer resynchronization method:

- **failover-protocol**—The tunnel uses the L2TP failover protocol method. If the peer non-failed endpoint does not support the L2TP failover protocol, a failover forces disconnection of the tunnel and all of its sessions.
- **failover-protocol-fallback-to-silent-failover**—The tunnel uses the L2TP failover protocol method; however, if the peer non-failed endpoint does not support the L2TP failover protocol method, the tunnel falls back to using the silent failover method.
- **silent-failover**—The tunnel uses the silent failover method. The tunnel also informs its peer that it supports the failover protocol method for the peer's failovers.
- **disable**—The tunnel does not use any peer resynchronization method for its own failovers, The tunnel informs its peer that it supports the failover protocol method for the peer's failovers. A failover forces the disconnection of the tunnel and all of its sessions.
- **not-configured**—Peer resynchronization is not configured for L2TP host profiles and AAA domain map tunnels. L2TP uses the global failover method.

By default, peer resynchronization is not configured at the L2TP profile-level or the domain map-level—therefore, the global configuration is used. This is different than using the **disable** keyword, which specifies that no peer synchronization method is used.

Use the **show l2tp destination profile** command to display a host profile's peer resynchronization configuration and the **show aaa domain-map** command to display a domain map's configuration.

- To configure peer resynchronization for an L2TP host profile:

```
host1(config)#l2tp destination profile lac-dest ip address 192.168.20.2
host1(config-l2tp-dest-profile)#remote host lac-host
host1(config-l2tp-dest-host-profile-host)#failover-resync silent-failover
```

- To configure peer resynchronization for an AAA domain map tunnel:

  host1(config)#**aaa domain-map lac-tunnel**
  host1(config-domain-map)#**tunnel 10**
  host1(config-domain-map-tunnel)#**failover-resync silent-failover**

Configuring the Global L2TP Peer Resynchronization Method

You can configure the peer resynchronization method globally, or for L2TP host profiles or domain map tunnels—a host profile or domain map tunnel configuration takes precedence over the global peer resynchronization configuration.

When you change the peer resynchronization method, the change is not immediately applied to existing tunnels. Tunnels continue using their current resynchronization method until the next time the tunnel is reestablished.

Use the **l2tp failover-resync** command to configure the global L2TP peer resynchronization method that L2TP failed endpoints use to resynchronize with a peer non-failed endpoint.

Choose one of the following keywords to specify the peer resynchronization method. All tunnels in the chassis use the specified method unless it is overridden by an L2TP host profile configuration or an AAA domain map configuration.

- **failover-protocol**—Tunnels use the L2TP failover protocol method. If the peer non-failed endpoint does not support the L2TP failover protocol, a failover forces disconnection of all tunnels and their sessions.
- **failover-protocol-fallback-to-silent-failover**—Tunnels use the L2TP failover protocol method; however, if the peer non-failed endpoint does not support the L2TP failover protocol method, the tunnel falls back to using the silent failover method.
- **silent-failover**—Tunnels use the silent failover method. The tunnels also inform their peers that they support the failover protocol method for peer failovers.
- **disable**—Tunnels do not use any peer resynchronization method for their own failovers. Tunnels inform their peers that they support the failover protocol method for peer failovers. A failover forces the disconnection of all tunnels and sessions.

Use the **show l2tp** command to display the global peer resynchronization configuration.

- To configure peer resynchronization for an L2TP host profile or AAA domain map tunnel:

  host1(config)#**l2tp failover-resync silent-failover**

- To restore the global default setting, which uses the **failover-protocol-fallback-to-silent-failover** method:

  host1(config)#**default l2tp failover-resync**

- To disable peer resynchronization, use the **no** version of the command—this is the same as using the **disable** keyword:

  host1(config)#**no l2tp failover-resync**

Using RADIUS to Configure Peer Resynchronization

The JUNOSe software supports the use of RADIUS to configure the L2TP peer resynchronization method used by your L2TP tunnels. You use the L2TP-Resynch-Method RADIUS attribute (VSA 26-90) in RADIUS Access-Accept messages to specify the L2TP peer resynchronization method.

Table 66 describes the L2TP-Resynch-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see *Chapter 3, Configuring RADIUS Attributes*. For more information about the L2TP-Resynch-Method attribute, see *Appendix 6, RADIUS Attribute Descriptions*.

Table 66: L2TP-Resynch-Method RADIUS Attribute

Standard Number	Attribute Name	Description	Length	Subtype Length	Value
[26-90]	L2TP-Resynch-Method	L2TP peer resynchronization method	12	6	integer: ■ 0 = disabled ■ 1 = failover protocol ■ 2 = silent failover ■ 3 = failover protocol with silent failover as backup

Related Topics

- **failover-resync** command
- **l2tp failover-resync** command

Configuring L2TP Tunnel Switch Profiles

You can use the **l2tp switch-profile** command to create an L2TP tunnel switch profile. An *L2TP tunnel switch profile* is a set of characteristics that defines the behavior of L2TP tunnel switching for the interfaces to which the profile is assigned.

Within the L2TP tunnel switch profile, you configure a particular tunnel switching behavior for a specified L2TP AVP. For example, you can configure the router to preserve the value of (relay) a specified AVP type across the LNS/LAC boundary in an L2TP tunnel-switched network.

Applying the L2TP Tunnel Switch Profile

Configuring an L2TP tunnel switch profile has no effect by itself. To use the tunnel switch profile in an L2TP tunnel-switched network, you must apply it to an L2TP outbound LAC session by using one of the following methods:

- Authentication, authorization, and accounting (AAA) domain maps
- AAA tunnel groups
- RADIUS Access-Accept messages

If none of these methods are used, you can apply the L2TP tunnel switch profile as an AAA default tunnel parameter. The default tunnel switch profile has lower precedence than the other methods for applying the tunnel switch profile.

For more information about the methods for applying L2TP tunnel switch profiles, see *Configuration Tasks* on page 331.

Configuration Guidelines

The following rules apply when you configure L2TP tunnel switch profiles:

- L2TP tunnel switching must be enabled for tunnel switch profiles to take effect. For information, see *Enabling Tunnel Switching on the Router* on page 332.
- L2TP tunnel switch profiles have no effect when they are assigned to a LAC session that is not tunnel switched.
- The router can relay only those AVPs that are accepted at the LNS. Malformed AVPs are never relayed.
- If a tunnel grant response specifies a named tunnel switch profile that has not been configured on the router, the router prohibits connection of the L2TP tunnel-switched session.
- If you remove a tunnel switch profile, the router also disconnects all associated L2TP switched sessions using that profile.
- In some cases, attributes configured in a tunnel switch profile take precedence over similar attributes configured globally on the router.

  For example, configuring L2TP Calling Number AVP 22 for relay overrides the **l2tp disable calling-number-avp** command issued from Global Configuration mode to prevent the router from sending AVP 22 in incoming-call-request (ICRQ) packets. In this scenario, the router relays the Calling Number AVP.

Configuring L2TP AVPs for Relay

Previously, the router did not preserve the values of incoming L2TP AVPs across the LNS/LAC boundary in an L2TP tunnel-switched network. The router regenerated most incoming AVPs, such as L2TP Calling Number AVP 22, based on the local policy in effect. However, some AVPs, such as Cisco NAS Port Info AVP 100, were dropped.

In an L2TP tunnel switch profile, you can define the types of AVPs that the router can relay unchanged across the LNS/LAC boundary. You can specify that the router relay one or more of the following AVP types:

- L2TP Bearer Type AVP 18
- L2TP Calling Number AVP 22
- Cisco NAS Port Info AVP 100

When you configure any of these AVP types for relay in an L2TP tunnel-switched network, the router preserves the value of an incoming AVP of this type when packets are switched between the inbound LNS session and the outbound LAC session.

Configuration Tasks

To configure and use an L2TP tunnel switch profile in an L2TP tunnel-switched network:

1. Ensure that L2TP tunnel switching is enabled on the router.
2. Configure the L2TP tunnel switch profile.
3. Apply the L2TP tunnel switch profile to the tunnel in one of the following ways:
   - To apply a named tunnel switch profile through an AAA domain map, use the **switch-profile** command from Domain Map Tunnel Configuration mode. For details, see *Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps* on page 333.
   - To apply a named tunnel switch profile through an AAA tunnel group, use the **switch-profile** command from Tunnel Group Tunnel Configuration mode. For details, see *Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups* on page 334.
   - To apply a named tunnel switch profile through RADIUS, include the Tunnel-Switch-Profile RADIUS attribute (VSA 26-91) in RADIUS Access-Accept messages. For details, see *Applying L2TP Tunnel Switch Profiles by Using RADIUS* on page 335.
   - To apply a default tunnel switch profile to a virtual router, use the **aaa tunnel switch-profile** command from Global Configuration mode. For details, see *Applying Default L2TP Tunnel Switch Profiles* on page 334.

The following sections describe how to perform each of these tasks.

Enabling Tunnel Switching on the Router

To enable L2TP tunnel switching on the router, use the **l2tp tunnel-switching** command. By default, tunnel switching is disabled.

- To enable L2TP tunnel switching:

  ```
  host1(config)#l2tp tunnel-switching
  ```

For more information, see *Enabling Tunnel Switching* on page 319.

Configuring L2TP Tunnel Switch Profiles

To configure an L2TP tunnel switch profile:

1. Create the L2TP tunnel switch profile and assign it a name. The **l2tp switch-profile** command accesses L2TP Tunnel Switch Profile Configuration mode.

   ```
   host1(config)#l2tp switch-profile concord
   host1(config-l2tp-tunnel-switch-profile)#
   ```

2. Configure the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. Use the **avp** command with the **relay** keyword to cause the router to preserve the value of an incoming AVP of this type when packets are switched between an inbound LNS session and an outbound LAC session.

   You can use any of the following keywords to specify the AVPs for the router to relay:

   - **bearer-type**—L2TP Bearer Type AVP 18; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy in effect
   - **calling-number**—L2TP Calling Number AVP 22; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy in effect
   - **cisco-nas-port**—Cisco NAS Port Info AVP 100; by default, the router drops this AVP

   Use the **no** version to restore the default L2TP tunnel switching behavior (regenerate or drop) for incoming AVPs of the specified type.

   The following commands configure the router to relay the Bearer Type, Calling Number, and Cisco NAS Port Info AVP types across the LNS/LAC boundary.

   ```
   host1(config-l2tp-tunnel-switch-profile)#avp bearer-type relay
   host1(config-l2tp-tunnel-switch-profile)#avp calling-number relay
   host1(config-l2tp-tunnel-switch-profile)#avp cisco-nas-port relay
   ```

3. (Optional) Use the **show l2tp switch-profile** command to verify configuration of the tunnel switch profile.

```
host1(config-l2tp-tunnel-switch-profile)#run show l2tp switch-profile
L2TP tunnel switch profile concord
L2TP tunnel switch profile myProfile
2 L2TP tunnel switch profiles found

host1(config-l2tp-tunnel-switch-profile)#run show l2tp switch-profile concord
L2TP tunnel switch profile concord
  AVP bearer type action is relay
  AVP calling number action is relay
  AVP Cisco nas port info action is relay
```

Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps

To apply an L2TP tunnel switch profile to sessions associated with an AAA domain map:

1. Access Domain Map Tunnel Configuration mode.

   host1(config)#**aaa domain-map westford.com**
   host1(config-domain-map)#**router-name default**
   host1(config-domain-map)#**tunnel 3**
   host1(config-domain-map-tunnel)#

   For more information about how to map a domain to an L2TP tunnel from Domain Map Tunnel Configuration mode, see *Mapping a User Domain Name to an L2TP Tunnel Overview* in *Chapter 12, Configuring an L2TP LAC*.

2. From Domain Map Tunnel Configuration mode, issue the **switch-profile** command to apply the specified L2TP switch profile to the sessions associated with this domain map.

   host1(config-domain-map-tunnel)#**switch-profile concord**

3. (Optional) Use the **show aaa domain-map** command to verify application of the tunnel switch profile.

```
host1(config-domain-map-tunnel)#run 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        <null>   <null>   l2tp     ipv4     <null>     <null>   <null>

         Tunnel                Tunnel                     Tunnel    Tunnel
Tunnel   Server     Tunnel       Max                      Virtual   Switch
 Tag      Name    Preference   Sessions     Tunnel RWS     Router    Profile
------   ------   ----------   --------   --------------   -------   -------
3        <null>   2000         0          system chooses   <null>    concord
```

Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups

To apply an L2TP tunnel switch profile to sessions associated with an AAA tunnel group:

1. Access Tunnel Group Tunnel Configuration mode.

   ```
   host1(config)#aaa tunnel-group sunnyvale
   host1(config-tunnel-group)#tunnel 3
   host1(config-tunnel-group-tunnel)#
   ```

   For more information about how to map a domain to an L2TP tunnel from Tunnel Group Tunnel Configuration mode, see *Mapping a User Domain Name to an L2TP Tunnel Overview* in *Chapter 12, Configuring an L2TP LAC*.

2. From Tunnel Group Tunnel Configuration mode, issue the **switch-profile** command to apply the specified L2TP switch profile to the sessions associated with this tunnel group.

   ```
   host1(config-tunnel-group-tunnel)#switch-profile sanjose
   ```

3. (Optional) Use the **show aaa tunnel-group** command to verify application of the tunnel switch profile.

   ```
   host1(config-tunnel-group-tunnel)#run show aaa tunnel-group

   Tunnel Group: sunnyvale
                                                                    Tunnel
   Tunnel   Tunnel   Tunnel   Tunnel   Tunnel    Tunnel    Tunnel   Client
    Tag      Peer    Source    Type    Medium   Password     Id      Name
   ------   ------   ------   ------   ------   --------   ------   ------
   3        <null>   <null>   l2tp     ipv4     <null>     <null>   <null>
            Tunnel                 Tunnel                      Tunnel    Tunnel
   Tunnel   Server     Tunnel       Max                        Virtual   Switch
    Tag      Name    Preference   Sessions     Tunnel RWS      Router    Profile
   ------   ------   ----------   --------   --------------   -------   -------
   3        <null>   2000         0          system chooses   <null>    sanjose
   ```

Applying Default L2TP Tunnel Switch Profiles

You can apply a default L2TP tunnel switch profile to a virtual router by issuing the **aaa tunnel switch-profile** command from Global Configuration mode. The router uses the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server *do not include* a named tunnel switch profile. The router ignores the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server *do include* a named tunnel switch profile.

The default L2TP tunnel switch profile applies to a specific virtual router. You can apply a different default tunnel switch profile to each virtual router configured.

To apply a default L2TP tunnel switch profile to a virtual router:

1. Create the virtual router to which you want to apply the default tunnel switch profile.

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

2. Issue the **aaa tunnel switch-profile** command to apply the default L2TP tunnel switch profile in the context of this virtual router.

   host1:east(config)#**aaa tunnel switch-profile boston**

3. (Optional) Use the **show aaa tunnel-parameters** command to verify application of the default tunnel switch profile.

```
host1:east(config)#run show aaa tunnel-parameters
Tunnel password is <NULL>
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch-profile is boston
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is descriptive
```

Applying L2TP Tunnel Switch Profiles by Using RADIUS

On the LAC, the router can receive tunnel configuration attributes through a RADIUS authentication server. To use RADIUS to apply an L2TP tunnel switch profile to a session, you can configure RADIUS to include the Tunnel-Switch-Profile RADIUS attribute (VSA 26-91) in RADIUS Access-Accept messages.

For more information about RADIUS Access-Accept messages, see *Chapter 3, Configuring RADIUS Attributes*. For more information about the Tunnel-Switch-Profile attribute, see *Chapter 6, RADIUS Attribute Descriptions*.

Related Topics

- Enabling Tunnel Switching on the Router on page 332
- Configuring L2TP Tunnel Switch Profiles on page 332
- Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps on page 333
- Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups on page 334
- Applying Default L2TP Tunnel Switch Profiles on page 334
- Applying L2TP Tunnel Switch Profiles by Using RADIUS on page 335
- **aaa tunnel switch-profile** command

- **avp** command
- **l2tp switch-profile** command
- **l2tp tunnel-switching** command

Configuring the Transmit Connect Speed Calculation Method

You can configure the method that the router uses to calculate the transmit connect speed of the subscriber's access interface for a tunneled L2TP session. L2TP reports the transmit connect speed in L2TP Transmit (TX) Speed AVP 24. During the establishment of an L2TP tunnel session, the LAC sends AVP 24 to the LNS to convey the transmit speed of the subscriber's access interface.

You can configure the calculation method for the transmit connect speed reported in L2TP Transmit (TX) Speed AVP 24 in any of the following ways. The first three methods—AAA domain maps, AAA tunnel groups, and RADIUS—are mutually exclusive.

- AAA domain maps—Use the **tx-connect-speed-method** command from Domain Map Tunnel Configuration mode. For instructions, see *Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method* on page 340.
- AAA tunnel groups—Use the **tx-connect-speed-method** command from Tunnel Group Tunnel Configuration mode. For instructions, see *Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method* on page 341.
- AAA default tunnel parameters—Use the **aaa tunnel tx-connect-speed-method** command from Global Configuration mode. The router uses the calculation method specified with this command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method.For instructions, see *Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method* on page 342.
- RADIUS—Include the Tunnel-Tx-Speed-Method RADIUS attribute (Juniper Networks VSA 26-94) in RADIUS Access-Accept messages. For instructions, see *Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method* on page 342.

Transmit Connect Speed Calculation Methods

In previous releases, the router calculated the transmit speed of the subscriber's access interface based only on statically configured settings for the underlying layer 2 access interface. With this feature, you can obtain a more accurate representation of the transmit connect speed by choosing a calculation method that reflects changes to the layer 2 interface due to statically configured settings, dynamically configured settings, or QoS settings.

You can choose one of the following methods for calculating the transmit connect speed that is reported in L2TP Transmit (TX) Speed AVP 24:

- Static layer 2
- Dynamic layer 2
- QoS
- Actual (lesser of dynamic layer 2 or QoS)

The following sections describe each of these calculation methods.

NOTE: Configuring the transmit connect speed calculation method has no effect on the operation of the L2TP Receive (RX) Speed AVP 38 or the Connect-Info RADIUS attribute [77] at the LAC.

Static Layer 2

The static layer 2 method calculates the transmit connect speed of the subscriber's access interface based on the statically configured settings for the underlying layer 2 ATM 1483 or Ethernet interface. The static layer 2 method does not reflect changes to the transmit speed of the layer 2 interface due to dynamically configured settings or to QoS.

For ATM 1483 circuits, the static layer 2 value is based on the bandwidth that the connection requires. The router uses certain traffic parameters for each service category to determine the required bandwidth for the connection. For more information about how the router computes bandwidth for ATM 1483 circuits, see *Connection Admission Control* in *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM*.

For Ethernet VLANs, the static layer 2 value is the advisory transmit speed of the VLAN subinterface, if configured with the **vlan advisory-tx-speed** command, or the speed of the underlying physical port if the advisory transmit speed is not configured.

If there is no explicit static configuration for the layer 2 interface, L2TP reports the speed of the underlying physical port as the transmit connect speed.

Dynamic Layer 2

The dynamic layer 2 method calculates the transmit connect speed of the subscriber's access interface based on the dynamically configured settings for the underlying layer 2 interface.

If there is no dynamic configuration for the layer 2 interface, L2TP reports the transmit connect speed based on statically configured settings. If there is no static speed configuration for the layer 2 interface, L2TP reports the speed of the underlying physical port as the transmit connect speed.

QoS

The QoS method calculates the transmit connect speed of the subscriber's access interface based on settings determined by static or dynamic QoS configurations. This calculation is based on the interface columns that QoS uses to build scheduler profiles for L2TP sessions. For example, a typical interface column might consist of an L2TP session over an Ethernet VLAN over a Gigabit Ethernet interface.

You can configure QoS to control the rate of any logical interface in the interface column. For those logical interfaces with a rate controlled by QoS, QoS reports this configured rate as the transmit connect speed for that interface. For those logical interfaces that do not have a QoS-configured rate, QoS reports the speed of the underlying physical port as the transmit connect speed.

For more information, see *QoS and L2TP TX Speed AVP 24 Overview* in *JUNOSe Quality of Service Configuration Guide, Chapter 22, Configuring QoS for L2TP Sessions*.

Actual

The actual method calculates the transmit connect speed of the subscriber's access interface as the lesser of the following two values:

- Value using the dynamic layer 2 calculation method
- Value using the QoS calculation method

Transmit Connect Speed Calculation Examples

The examples in this section illustrate how the router uses the methods described in *Transmit Connect Speed Calculation Methods* on page 336 to calculate the transmit connect speed.

Example 1: L2TP Session over ATM 1483 Interface

In this example, an L2TP session is established over an ATM 1483 subinterface on an OC3/STM1 ATM IOA. The configuration has the following characteristics:

- There is no explicit static configuration for the layer 2 (ATM 1483) interface.
- A transmit connect speed of 10 Mbps is provided dynamically from a RADIUS authentication server when the subscriber logs in.
- The transmit connect speed calculated by QoS is 5 Mbps.

Based on these characteristics, Table 67 lists the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 for each calculation method, and the reason why L2TP reports this value.

Table 67: Transmit Connect Speeds for L2TP over ATM 1483 Example

Calculation Method	Transmit Connect Speed Reported in AVP 24	Reason
Static layer 2	155 Mbps	L2TP reports the speed of the underlying OC3 physical port because there is no explicit static configuration for the layer 2 interface.
Dynamic layer 2	10 Mbps	L2TP reports the transmit connect speed provided by RADIUS.
QoS	5 Mbps	L2TP reports the transmit connect speed calculated by QoS.
Actual	5 Mbps	L2TP reports the lesser of the dynamic layer 2 speed (10 Mbps) or the QoS speed (5 Mbps).

Example 2: L2TP Session over Ethernet VLAN Interface

In this example, an L2TP session is established over a PPPoE subinterface over an Ethernet VLAN subinterface. The configuration has the following characteristics:

- The Ethernet VLAN subinterface is configured with an advisory transmit speed of 100 Mbps.
- The dynamic layer 2 setting does not apply to the VLAN subinterface.
- The transmit connect speed calculated by QoS is 10 Mbps.

Based on these characteristics, Table 68 lists the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 for each calculation method, and the reason why L2TP reports this value.

Table 68: Transmit Connect Speeds for L2TP over Ethernet Example

Calculation Method	Transmit Connect Speed Reported in AVP 24	Reason
Static layer 2	100 Mbps	L2TP reports the advisory transmit speed configured on the VLAN subinterface. If configured, the advisory transmit speed takes precedence over the physical port speed for a VLAN subinterface.
Dynamic layer 2	100 Mbps	L2TP reports the static layer 2 value because the dynamic layer 2 setting does not apply to a VLAN subinterface.
QoS	10 Mbps	L2TP reports the transmit connect speed calculated by QoS.
Actual	10 Mbps	L2TP reports the lesser of the dynamic layer 2 speed (100 Mbps) or the QoS speed (10 Mbps).

Transmit Connect Speed Reporting Considerations

The following considerations affect the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 when you use this feature.

Session Termination for Dynamic Speed Timeout

Under certain heavy load conditions, the router might be unable to obtain the dynamic-layer2 value for the transmit connect speed of the subscriber's access interface. In this situation, the LAC sends the LNS an L2TP Call-Disconnect-Notify (CDN) message to terminate the L2TP session.

For more information about supported L2TP terminate reasons, see *Chapter 7, Application Terminate Reasons*.

Advisory Speed Precedence for VLANs over Bridged Ethernet

For interface columns that consist of an L2TP session over an Ethernet VLAN subinterface over a bridged Ethernet interface, the advisory transmit speed of the VLAN subinterface, if configured with the **vlan advisory-tx-speed** command, takes precedence over the physical port speed of the underlying layer 2 ATM 1483 interface. As a result, if the advisory transmit speed is configured for the VLAN subinterface, L2TP reports this value as the transmit connect speed regardless of the port speed of the ATM 1483 interface.

Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method

To configure the transmit connect speed calculation method for a tunneled L2TP session associated with an AAA domain map:

1. Access Domain Map Tunnel Configuration mode.

   ```
   host1(config)#aaa domain-map sunnyvale.com
   host1(config-domain-map)#router-name lac
   host1(config-domain-map)#tunnel 5
   host1(config-domain-map-tunnel)#
   ```

   For more information about how to map a domain to an L2TP tunnel from Domain Map Tunnel Configuration mode, see *Mapping a User Domain Name to an L2TP Tunnel Overview* in *Chapter 12, Configuring an L2TP LAC*.

2. From Domain Map Tunnel Configuration mode, configure the calculation method for the transmit connect speed of the subscriber's access interface.

   ```
   host1(config-domain-map-tunnel)#tx-connect-speed-method dynamic-layer2
   ```

3. (Optional) Use the **show aaa domain-map** command to verify configuration of the transmit connect speed calculation method.

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

   Domain: sunnyvale.com; router-name: lac; ipv6-router-name: default
                                                                    Tunnel
   Tunnel   Tunnel   Tunnel   Tunnel   Tunnel    Tunnel    Tunnel   Client
    Tag      Peer    Source    Type    Medium   Password     Id      Name
   ------   ------   ------   ------   ------   --------   ------   ------
   5        <null>   <null>   l2tp     ipv4     <null>     <null>   <null>
   ```

```
         Tunnel                  Tunnel                      Tunnel
Tunnel   Server      Tunnel       Max                         Virtual
 Tag      Name     Preference   Sessions     Tunnel RWS       Router
------   ------   ----------   --------   --------------   -------
5        <null>   2000         0          system chooses   <null>
          Tunnel    Tunnel        Tunnel
Tunnel   Failover   Switch          Tx
 Tag      Resync    Profile     Speed Method
------   --------   -------   --------------
5        <null>     <null>    dynamic layer2
```

Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method

To configure the transmit connect speed calculation method for a tunneled L2TP session associated with an AAA tunnel group:

1. Access Tunnel Group Tunnel Configuration mode.

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

   For more information about how to map a domain to an L2TP tunnel from Tunnel Group Tunnel Configuration mode, see *Mapping a User Domain Name to an L2TP Tunnel Overview* in *Chapter 12, Configuring an L2TP LAC*.

2. From Tunnel Group Tunnel Configuration mode, configure the calculation method for the transmit connect speed of the subscriber's access interface.

   host1(config-tunnel-group-tunnel)#**tx-connect-speed-method qos**

3. (Optional) Use the **show aaa tunnel-group** command to verify configuration of the transmit connect speed calculation method.

   ```
   host1(config-tunnel-group-tunnel)#run show aaa tunnel-group

   Tunnel Group: boston
                                                                    Tunnel
   Tunnel   Tunnel   Tunnel   Tunnel   Tunnel    Tunnel    Tunnel   Client
    Tag      Peer    Source    Type    Medium   Password     Id      Name
   ------   ------   ------   ------   ------   --------   ------   ------
   3        <null>   <null>   l2tp     ipv4     <null>     <null>   <null>
            Tunnel                 Tunnel                      Tunnel
   Tunnel   Server     Tunnel       Max                         Virtual
    Tag      Name    Preference   Sessions     Tunnel RWS       Router
   ------   ------   ----------   --------   --------------   -------
   3        <null>   2000         0          system chooses   <null>
                                  Tunnel
             Tunnel    Tunnel      Tx
   Tunnel   Failover   Switch    Speed
    Tag      Resync    Profile   Method
   ------   --------   -------   ------
   3        <null>     <null>    qos
   ```

Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method

You can configure the transmit connect speed calculation method as a default AAA tunnel parameter by using the **aaa tunnel tx-connect-speed-method** command from Global Configuration mode. This command applies the specified calculation method to all tunneled L2TP sessions associated with a particular virtual router, and thereby alleviates the need for you to configure the transmit connect speed calculation method for each individual subscriber.

Configuring the calculation method as a default AAA tunnel parameter for a virtual router has lower precedence than using AAA domain maps, AAA tunnel groups, or RADIUS to configure the transmit connect speed calculation method. The router uses the calculation method specified with the **aaa tunnel tx-connect-speed-method** command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method.

To configure the transmit connect speed calculation method for all tunneled L2TP sessions associated with a particular virtual router:

1. Create the virtual router for which you want to configure the transmit connect speed calculation method.

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

   For more information about configuring and using virtual routers, see *JUNOSe System Basics Configuration Guide, Chapter 13, Configuring Virtual Routers*.

2. Configure the transmit connect speed calculation method in the context of this virtual router.

   host1:north(config)#**aaa tunnel tx-connect-speed-method qos**

   - To specify the calculation method for the transmit connect speed, use one of the following keywords, as described in *Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method* on page 341:
     - **static-layer2**
     - **dynamic-layer2**
     - **qos**
     - **actual**

3. (Optional) Use the **show aaa tunnel-parameters** command to verify configuration of the transmit connect speed calculation method.

```
host1:north(config)#run show aaa tunnel-parameters
Tunnel password is <NULL>
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch-profile is boston
Tunnel tx-connect-speed-method is qos
```

```
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is fixed
```

Using RADIUS to Configure the Transmit Connect Speed Calculation Method

On the LAC, the router can receive tunnel configuration attributes through a RADIUS authentication server. To use RADIUS to configure the transmit connect speed calculation method for a subscriber's access interface, you can configure RADIUS to include the Tunnel-Tx-Speed-Method RADIUS attribute (Juniper Networks VSA 26-94) in RADIUS Access-Accept messages.

Table 69 describes the Tunnel-Tx-Speed-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see *Chapter 3, Configuring RADIUS Attributes*. For a description of the RADIUS attributes supported by JUNOSe software, see *Chapter 6, RADIUS Attribute Descriptions*.

Table 69: Tunnel–Tx-Speed-Method RADIUS Attribute

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-94]	Tunnel-Tx-Speed-Method	The method that the router uses to calculate the transmit connect speed of the subscriber's access interface	12	6	integer: ■ 1 = static-layer2; TX speed based on static layer 2 settings ■ 2 = dynamic-layer2; TX speed based on dynamic layer 2 settings ■ 3 = qos; TX speed based on QoS settings ■ 4 = actual; TX speed that is the lesser of the dynamic-layer2 value or the qos value

Related Topics

- Transmit Connect Speed Calculation Methods on page 336
- Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method on page 340
- Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method on page 341
- Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method on page 342
- Using RADIUS to Configure the Transmit Connect Speed Calculation Method on page 343
- **aaa tunnel tx-connect-speed-method** command
- **tx-connect-speed-method** command

PPP Accounting Statistics

JUNOSe accounting for tunneled subscribers at the L2TP LAC counts the payload that PPP passes to or receives from L2TP for transport. At this stage in the protocol processing, any padding outside PPP, such as that for PPPoE, has been removed. Accounting includes the authentication acknowledgement packet, CHAP success packets, and PAP acknowledgment packets. Accounting ends when L2TP has been notified to terminate the session. The statistics are reported in the following RADIUS attributes:

Attribute Number	Attribute Name
42	Acct-Input-Octets
43	Acct-Output-Octets
47	Acct-Input-Packets
48	Acct-Output-Packets

Termination of a tunneled session can result from PPP termination, L2TP shutdown, subscriber logout, or lower layer down events. When the session is terminated through PPP, the software counts both the PPP terminate-request and the PPP terminate-acknowledgement packets.

- Accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) for tunneled PPP customers at the L2TP LAC include the following data:
  - All upper layer control traffic, including IPCP, IPCPv6, OSICP, and MPLSNCP
  - All data traffic, including IP, IPv6, MPLS, and OSI
  - PPP PAP or CHAP acknowledgments. and also retransmission of PAP or CHAP that take place after the session is active (even when proxy authentication is accepted)
  - All PPP PAP or CHAP negotiations in the case where proxy authentication is disabled or required to renegotiate at the LNS
  - All LCP traffic when proxy LCP is disabled or required to renegotiate at the LNS
  - All PPP LCP echo requests and their responses
  - PPP LCP terminate-request or terminate-acknowledgement packets from the client or LNS when PPP initiates termination of the session
  - If present, the two PPP header bytes (Address Field 0xFF and Control Field 0x03) as part of the L2TP payload

- Accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) for tunneled PPP customers at the L2TP LAC exclude the following data:
  - LCP when Proxy LCP is enabled and accepted at the LNS
  - Initial PPP PAP request
  - Initial PPP CHAP challenge and response
- Accounting statistics reported in RADIUS packet counts (Acct-Input-Packets and Acct-Output-Packets) for tunneled PPP customers at the L2TP LAC are based on packets delivered to or received from the L2TP session. These statistics exclude L2TP control traffic and L2TP hello messages.

For information on accounting statistics for terminated PPP sessions, see *PPP Accounting Statistics* in *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol*.